Till statsrådet och chefen för Justitiedepartementet

Den 20 december 2002 beslutade chefen för Justitiedepartementet att uppdra åt överåklagaren Gunnel Lindberg att utarbeta en promemoria som behandlar frågan om Sveriges tillträde till och genomförande i svensk rätt av Europarådets konvention om brott i cyberrymden.

Uppdraget har under hand utökats till att omfatta även det tilläggsprotokoll till konventionen som upprättades den 28 januari 2003.

Härmed överlämnas promemorian Brott och brottsutredning i IT-miljö; Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll.

Uppdraget är därmed slutfört.

Stockholm i februari 2005.

Gunnel Lindberg

Innehåll

1 Sammanfattning

Bakgrund

Sverige undertecknade den 23 november 2001 Europarådets konvention om IT-relaterad brottslighet och den 28 januari 2003 ett tilläggsprotokoll till denna. Promemorian behandlar frågan om konventionen och protokollet bör ratificeras av Sverige. I promemorian läggs fram de förslag till de lagändringar som krävs för en anpassning till konventionen.

I kapitel 4 redovisas konventionens huvudsakliga innehåll. Konventionen har tre huvudsyften. Det första är att åstadkomma en harmonisering av den nationella straffrätten beträffande vissa gärningar som behandlas i konventionen, om de begås med hjälp av datorsystem. Gärningarna är följande:
- olagligt intrång i datorsystem,
- olovlig avlyssning av datorbehandlingsbara uppgifter och av elektromagnetiska emissioner från datorer och datorsystem,
- datastörning,
- systemstörning,
- missbruk av hjälpmedel som kan användas för nu nämnda typer av brott,
- datarelaterad förfalskning,
- datarelaterat bedrägeri,
- barnpornografi samt
- intrång i upphovsrätt och i närstående rättigheter.

Det andra huvudsyftet med konventionen är att få fram nationella processrättsliga bestämmelser som tillgodoser behoven av
- att utreda och lagföra de brott som behandlas i konventionen

- att utreda och lagföra andra IT-relaterade brott och andra brott som begås med hjälp av datorer samt
- att kunna ta till vara bevisning i elektronisk form i brottmål.

Det tredje huvudsyftet med konventionen är att lägga grunden för ett effektivt internationellt samarbete vid bekämpningen av IT-relaterade brott.

I kapitel 5 redogörs för innehållet i tilläggsprotokollet, som enbart behandlar frågan om ansvar för och utredning av gärningar av rasistisk och främlingsfientlig natur som begås med hjälp av datorsystem.

Kapitel 6 innehåller en jämförelse mellan kraven i konventionen och den svenska lagstiftningen. I de flesta hänseenden uppfyller den svenska lagstiftningen redan de krav som konventionen ställer. I några avseenden saknas det emellertid regler som täcker åtagandena i konventionen och i andra fall krävs det vissa justeringar av den befintliga lagstiftningen.

På motsvarande sätt görs i kapitel 7 en jämförelse mellan åtagandena i tilläggsprotokollet och den svenska lagstiftningen. Bedömningen är att tilläggsprotokollet inte i sig bör föranleda några lagstiftningsåtgärder.

I kapitel 8 finns en redogörelse för arbetet i andra länder med att genomföra konventionen och tilläggsprotokollet.

Bör konventionen och tilläggsprotokollet ratificeras?

Kapitel 9 behandlar frågan om konventionen respektive tilläggsprotokollet bör ratificeras.

Sverige har länge intagit en ledande position såväl i fråga om lagstiftning på IT-området som i fråga om hög grad av datoranvändning. Det är därför viktigt med en strafflagstiftning som ger ett gott skydd mot missbruk av den moderna tekniken och en processlagstiftning som ger goda möjligheter att utreda och lagföra IT-relaterade brott. Det är också viktigt att Sverige deltar aktivt i det internationella samarbetet med bekämpning av brottslighet av detta slag, eftersom ett utmärkande drag för denna är att den inte hindras av landgränser.

Mot den nu angivna bakgrunden föreslås att såväl konventionen som tilläggsprotokollet ratificeras.

Förslag till lagändringar

Allmänt om förslagen

I kapitel 10 redovisas vilka förslag till lagändringar som har lagts fram som ett led i genomförande av EU-rambeslutet om angrepp mot informationssystem. Eftersom rambeslutet och konventionen i fråga om några artiklar ansluter mycket nära till varandra bygger förslagen i denna promemoria vidare på de ändringsförslag som redan har presenterats.

Kapitel 11 innehåller förslagen till lagändringar. Förslagen rör två huvudområden; straffrättsliga regler och processrättsliga regler. Vidare föreslås det en rad ändringar i lagen om internationell rättslig hjälp, som har till syfte att ge de nya processrättsliga reglerna nödvändigt lagstöd så att de kan användas i det internationella samarbetet på det rättsliga området. Även i lagen om elektronisk kommunikation föreslås ändringar i syfte att anpassa bestämmelserna till de nya processrättsliga reglerna. Dessutom föreslås att operatörernas skyldighet att utan hinder av tystnadsplikten lämna uppgifter om trafikdata till brottsbekämpande myndigheter utvidgas. Vidare föreslås vissa följdändringar i några andra lagar.

Ändringar inom straffrätten

De ändringar och utvidgningar i straffansvaret för dataintrång som redan har föreslagits som ett led i genomförandet av EU-rambeslutet om angrepp på informationssystem täcker i allt väsentligt det som krävs för att uppfylla kraven i konventionen på kriminalisering av gärningar som innebär intrång i eller påverkan på informationssystem eller datorbehandlingsbara uppgifter.

Några ytterligare lagändringar på det området föreslås därför inte.

Däremot föreslås det att olovlig avlyssning av elektromagnetiska emissioner och andra signaler till, från eller inom en dator eller ett datorsystem straffbeläggs, eftersom nuvarande straffbestämmelser inte täcker hela det område som enligt konventionen skall vara kriminaliserat. Endast avlyssning med tekniska hjälpmedel straffbeläggs. Det skall vidare vara fråga om avlyssning av signaler som inte är allmänt tillgängliga. Den nya bestämmelsen placeras i paragrafen om dataintrång. Förberedelse till olovlig avlyssning av datorer straffbeläggs i en särskild paragraf.

Straffansvaret för förfalskning tar sikte på traditionella urkunder. Eftersom en översyn av 14 och 15 kap. brottsbalken har aviserats förslås det att anpassningen till konventionen inskränks till enbart ändringar som är oundgängligen nödvändiga, för att inte föregripa framtida överväganden. Därför föreslås inte någon ändring i urkundsbegreppet. I stället utvidgas straffansvaret för brukande av något som är förfalskat till att gälla även åberopande av icke autentiska sammanställningar av elektroniska data, om gärningen innebär fara i bevishänseende.

Ändringar inom processrätten

Tyngdpunkten i förslagen ligger på det processrättsliga området. Inledningsvis konstateras det att bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning är av avgörande betydelse för hur det nuvarande regelsystemet skall anpassas till konventionen. Detta beror på att datakommunikation som förmedlas via kommunikationsnät i svensk lagstiftning betraktas som telemeddelanden. Eftersom statsmakterna nyligen har slagit fast att nyss nämnda tvångsmedel är exklusivt tillämpliga för bevissäkring hos operatörer måste de nya reglerna utgå från detta.

För att bevisning om datakommunikation skall kunna säkras snabbare än vad som nu är fallet föreslås det att ett nytt tvångsmedel införs. Tvångsmedlet, som kallas frysning av elektronisk

kommunikation, skall utgöra ett förstadium till hemlig teleavlyssning och hemlig teleövervakning. Det skall beslutas av åklagare. Förutsättningarna för att använda tvångsmedlet skall vara desamma som för hemlig teleavlyssning och hemlig teleövervakning. Frysning av elektronisk kommunikation har endast den verkan att operatörerna tillfälligt skall bevara uppgifter om kommunikationen, i avvaktan på att domstol tar ställning till användningen av hemliga tvångsmedel. Först efter domstolsbeslut får uppgifterna om innehållet i eller omständigheterna kring kommunikationen lämnas ut. Åklagaren skall mycket snabbt efter ett frysningsbeslut underställa domstol frågan om användning av hemliga tvångsmedel.

Det föreslås också en ny typ av tvångsåtgärd, förbud mot att rubba bevisning i elektronisk form. Syftet med åtgärden är att temporärt förbjuda den som innehar bevisning i elektronisk form att förstöra, förändra eller på annat sätt göra bevisningen oåtkomlig. Förbudet har formen av ett föreläggande som meddelas av åklagare. Ett sådant föreläggande får inte riktas mot någon som är misstänkt och får heller inte avse något som inte får tas i beslag. Förbudet skall förenas med skyldighet att bevara bevisningen viss tid, högst 90 dagar. Förbudet kan förlängas genom ett nytt beslut. Åklagaren får också förbjuda den som har fått ett sådant föreläggande att yppa detta. Den som har drabbats av ett förbud kan begära rättens prövning av det. För sådan prövning skall gälla samma regler som för prövning av beslag.

Reglerna om husrannsakan och beslag anpassas till den moderna tekniken. I rättegångsbalken införs en ny regel om husrannsakan i IT-miljö. Förutsättningarna för en sådan husrannsakan skall i princip vara desamma som för husrannsakan i en fysisk miljö. Kretsen som får besluta om husrannsakan i IT-miljö blir dock något snävare än kretsen som kan besluta om en vanlig husrannsakan. Vidare skall enligt förslaget husrannsakan i IT-miljö i vissa fall kunna verkställas via kommunikationsnät.

Genom ändringar i reglerna om beslag görs det klart att beslag kan avse information i elektronisk form. Ändringarna innebär bl.a. att de s.k. beslagsförbuden, som hindrar beslag av särskilt

integritetskänsliga handlingar, görs direkt tillämpliga på elektronisk information. Reglerna om edition ändras på motsvarande sätt.

Vidare införs det en möjlighet att hålla kvar elektronisk post för eventuellt beslag. Bestämmelsen utformas efter mönster av regeln om kvarhållande av brev och försändelser av traditionellt slag. Samma rättsliga förutsättningar som för kvarhållande av traditionell post skall gälla för kvarhållande av elektronisk post. Beslut om kvarhållande skall meddelas av domstol.

Det föreslås också att det nuvarande undantaget för hemlig teleavlyssning (och hemlig teleövervakning) av telenät av mindre betydelse görs snävare. Endast telenät som saknar betydelse ur allmän kommunikationssynpunkt undantas.

Ändringar i lagen om elektronisk kommunikation

En ny regel om röjande av trafikuppgifter införs i lagen om elektronisk kommunikation. En operatör skall på begäran röja trafikuppgifter beträffande ett särskilt utpekat meddelande, om uppgifterna behövs för att spåra den väg på vilket meddelandet överfördes och den eller de operatörer som medverkade i överföringen. Sådana uppgifter får röjas endast om det är fråga om ett brott med fängelse ett år i straffskalan. Uppgifterna får bara röjas för polisen eller för en åklagare.

Förslagen om frysning av elektronisk kommunikation och kvarhållande av elektronisk post kräver vissa följdändringar i lagen om elektronisk kommunikation. Dessa tvångsmedel verkställs i samverkan mellan Säkerhetspolisen och en teleoperatör. Reglerna om teleoperatörers tystnadsplikt och anpassningsskyldighet kompletteras med bestämmelser om de nya tvångsmedlen.

Nya regler om internationell rättslig hjälp

En förutsättning för att de nya processrättsliga reglerna skall få genomslag i det internationella samarbetet är att dessa har sin motsvarighet i regler i lagen om internationell rättslig hjälp.

Det föreslås därför att uppräkningen i 2 kap. 1 § i lagen om internationell rättslig hjälp, som uttömmande anger vilka tvångsmedel som får användas på begäran av främmande stat, kompletteras. I uppräkningen skall de nya tvångsmedlen frysning av elektronisk kommunikation, förbud mot att rubba bevisning i elektronisk form och kvarhållande av elektronisk post anges. Det krävs dubbel straffbarhet för hjälp med frysning av elektronisk kommunikation och kvarhållande av elektronisk post. I princip krävs det dubbel straffbarhet även för hjälp med förbud att rubba elektronisk bevisning. I förhållande till vissa länder är dock det kravet uppmjukat, på samma sätt som gäller för beslag. Vidare görs en justering av uppräkningen av tvångsmedel som får användas på begäran av annan stat, så att även kvarhållande av försändelse kan användas vid rättslig hjälp.

Även den nya regeln i lagen om elektronisk kommunikation om röjande av trafikuppgifter anges som ett instrument som får användas vid internationell rättslig hjälp.

I lagen införs också regler om förfarandet vid rättslig hjälp med de nya instrumenten.

En svensk åklagare ges rätt att i en annan stat begära rättslig hjälp med åtgärder som svarar mot de föreslagna utvidgningarna.

Övriga lagändringar

I två andra lagar, som också innehåller regler om hemlig teleavlyssning och hemlig teleövervakning, görs följdändringar med anledning av att reglerna om frysning av elektronisk kommunikation skall vara generellt tillämpliga.

Det föreslås också att de nya hemliga tvångsmedlen (frysning av elektronisk kommunikation och kvarhållande av elektronisk post) skall kringgärdas med samma undantag från meddelarfri-

heten som i dag gäller för hemliga tvångsmedel på teleområdet och för kvarhållande av traditionell post.

Kostnader, genomförande m.m.

Förslagen, som bedöms kunna finansieras inom befintliga ekonomiska ramar, bör genomföras så snart som möjligt.

I fråga om de straffrättsliga ändringarna föreslås övergångsbestämmelser som innebär att reglerna endast skall kunna tillämpas på brott som har begåtts efter ikraftträdandet. För övriga lagändringar föreslås inga övergångsbestämmelser.

2 Författningsförslag

2.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken

dels att 9 kap. 6 §, 27 kap. 1, 3, 9, 15, 20 och 21§§, 28 kap. 4-7 §§, 38 kap. 2 § samt 39 kap. 5 § skall ha följande lydelse,

dels att det skall införas tre nya paragrafer, 27 kap. 9 a och 21 a §§ samt 28 kap. 1 a § av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 kap.	
6 §[1]	
Röjer någon utan giltigt skäl *vad* enligt rättens eller undersökningsledarens förordnande inte får uppenbaras, döms han till böter.	Röjer någon utan giltigt skäl *något som* enligt rättens, *åklagarens* eller undersökningsledarens förordnande inte får uppenbaras, döms han till böter.
27 kap.	
1 §[2]	
Föremål, som skäligen kan *antagas äga* betydelse för utredning om brott eller vara genom brott *någon avhänt* eller på grund av brott *förverkat*, *må*	Föremål, som skäligen kan *antas ha* betydelse för utredning om brott eller vara *avhänt någon* genom brott eller *förverkat* på grund av brott, *får tas*

[1] Senaste lydelse 1991:241.
[2] Senaste lydelse 1989:650.

tagas i beslag.	i beslag.
Vad i detta kapitel *stadgas* om föremål *gälle ock, i den mån ej* annat är föreskrivet, *om skriftlig handling*.	*Bestämmelserna* i detta kapitel om föremål *gäller även skriftlig handling och elektronisk upptagning, om inte annat är föreskrivet. Vad som i kapitlet sägs om skriftlig handling skall gälla även för elektronisk upptagning av skrift.*

Tvångsmedel enligt detta kapitel får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse.

3 §[3]

Brev, telegram eller annan försändelse, som finns hos ett post- eller telebefordringsföretag, får tas i beslag endast om det för brottet är föreskrivet fängelse i ett år eller däröver och försändelsen hade kunnat tas i beslag hos mottagaren.

Vad som sägs i första stycket gäller även meddelande som avses i 9 a §.

9 §[4]

Rätten får *förordna*, att försändelse som får tas i beslag och som väntas komma in till ett befordringsföretag skall, när försändelsen kommer in, hållas kvar till dess frågan om beslag har avgjorts. Fråga därom får tas upp endast på yrkande av *undersökningsledaren eller* åklagaren.	Rätten får *besluta*, att försändelse som får tas i beslag och som väntas komma in till ett befordringsföretag skall, när försändelsen kommer in, hållas kvar till dess frågan om beslag har avgjorts. Fråga därom får tas upp endast på yrkande av åklagaren.

[3] Senaste lydelse 1993:602.
[4] Senaste lydelse 1993:602.

Ett *förordnande* skall meddelas att gälla för viss tid, högst en månad, från den dag då *förordnandet* delgavs befordringsföretaget. I *förordnandet* skall det tas in en underrättelse om att meddelande om åtgärden inte utan tillstånd av *undersökningsledaren* får lämnas till avsändaren, mottagaren eller någon annan.

När en försändelse *på grund av ett förordnande* hållits kvar, skall befordringsföretaget utan dröjsmål *göra anmälan hos den som har begärt förordnandet*. Denne skall omedelbart pröva, om beslag skall ske.

Ett *beslut om kvarhållande* skall meddelas att gälla för viss tid, högst en månad, från den dag då *beslutet* delgavs befordringsföretaget. *Tiden får inte bestämmas längre än nödvändigt.* I *beslutet* skall det tas in en underrättelse om att meddelande om åtgärden inte utan tillstånd av *åklagaren* får lämnas till avsändaren, mottagaren eller någon annan.

När en försändelse har hållits kvar *med stöd av denna paragraf*, skall befordringsföretaget utan dröjsmål *anmäla detta till åklagaren.* Denne skall omedelbart pröva, om beslag skall ske.

Om det inte längre finns skäl för ett beslut om kvarhållande skall åklagaren eller rätten omedelbart häva beslutet.

9 a §

För ändamål som anges i 9 § får rätten, på yrkande av åklagaren, besluta att telemeddelande som väntas komma in till en adress för elektronisk post och som får tas i beslag hos mottagaren får hållas kvar till dess frågan om beslag har avgjorts.

Ett beslut om kvarhållande skall meddelas att gälla för viss tid. Tiden får inte bestämmas

längre än nödvändigt och får inte överstiga en månad från dagen för beslutet.

Vad som sägs i 9 § andra stycket tredje meningen och tredje stycket skall i tillämpliga delar gälla kvarhållande av telemeddelande. Vad som sägs om befordringsföretag skall i stället gälla skall den som tillhandahåller en sådan allmänt tillgänglig kommunikationstjänst som regleras i 6 kap. lagen om elektronisk kommunikation.

Med telemeddelande avses ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.

Om det inte längre finns skäl för ett beslut om kvarhållande skall åklagaren eller rätten omedelbart häva beslutet.

15 §

För säkerställande av utredning om brott *må* byggnad eller rum *tillstängas*, tillträde till visst område förbjudas, förbud meddelas mot flyttande av visst föremål eller annan dylik åtgärd *vidtagas*.

Om *åtgärd, som nu nämnts*, *gälle* i tillämpliga delar vad i

För säkerställande av utredning om brott *får* byggnad eller rum *stängas till*, tillträde till visst område förbjudas, förbud meddelas mot flyttande av visst föremål eller annan dylik åtgärd *vidtas*.

Om *åtgärder enligt första stycket gäller* i tillämpliga delar

detta kapitel är *stadgat* om beslag.	vad i detta kapitel är *föreskrivet* om beslag.
	För ändamål som anges i första stycket får en åklagare förbjuda den som innehar data i elektronisk form att förstöra, förändra eller på annat sätt göra dessa oåtkomliga, om det finns särskild risk att de annars går förlorade. Ett sådant förbud får inte riktas mot någon som är misstänkt eller avse något som inte får tas i beslag hos innehavaren. Förbudet skall förenas med skyldighet att bevara uppgifterna i högst 90 dagar. Tiden får inte bestämmas längre än nödvändigt.
	Åklagaren får förordna att den som ålagts ett förbud enligt tredje stycket inte får uppenbara detta. När förbudet upphör genom beslut av åklagare om beslag eller annat tvångsmedel skall denne ta ställning till om förordnandet att inte uppenbara förbudet skall bestå.
	Den som har drabbats av ett förbud enligt tredje stycket får begära rättens prövning av förbudet. För sådan prövning gäller 6 § i tillämpliga delar.

20 §[5]

Hemlig teleavlyssning och hemlig teleövervakning får ske endast om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

1. en teleadress som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte, eller

2. en teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta.

Avlyssning eller övervakning får inte avse telemeddelanden som endast befordras eller har befordrats inom ett *telenät* som med hänsyn till sin begränsade omfattning och omständigheternas i övrigt får anses *vara av mindre* betydelse från allmän kommunikationssynpunkt.

Avlyssning eller övervakning får inte avse telemeddelanden som endast befordras eller har befordrats inom ett *kommunikationsnät* som med hänsyn till sin begränsade omfattning och omständigheternas i övrigt får anses *sakna* betydelse från allmän kommunikationssynpunkt.

21 §[6]

Frågor om hemlig teleavlyssning och hemlig teleövervakning prövas av rätten på ansökan av åklagaren.

I ett beslut att tillåta hemlig teleavlyssning eller hemlig teleövervakning skall det anges vilken teleadress och vilken tid tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen

I ett beslut att tillåta hemlig teleavlyssning eller hemlig teleövervakning skall det anges vilken teleadress och vilken tid tillståndet avser *samt om tillståndet omfattar uppgifter som varit föremål för åtgärd enligt 21 a §.* Tiden får inte bestämmas längre än nödvändigt och

[5] Senaste lydelse 2003:1146.
[6] Senaste lydelse 2003:1146.

för beslutet.	får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.
I tillstånd till avlyssning eller övervakning skall det särskilt anges om åtgärden får verkställas utanför *allmänt tillgängliga telenät*.	I tillstånd till avlyssning eller övervakning skall det särskilt anges om åtgärden får verkställas utanför *allmänna kommunikationsnät*.
	21 a §
	I avvaktan på rättens beslut i fråga om åtgärd enligt 18 eller 19 § får en åklagare, om det föreligger fara i dröjsmål, besluta om frysning av elektronisk kommunikation. Frysning innebär att uppgifter angående telemeddelanden eller innehållet i sådana meddelanden skall bevaras i avvaktan på domstols beslut i fråga om hemlig teleavlyssning eller hemlig teleövervakning. Vad som sägs i 18, 19, 21 § andra och tredje styckena och 22 § gäller för beslut om frysning av elektronisk kommunikation.
	Har en åklagare beslutat om frysning av elektronisk kommunikation skall han snarast och senast andra dagen efter beslutet ge in en framställning till rätten om hemlig teleavlyssning eller hemlig teleövervakning. Görs inte detta skall åklagaren omedelbart häva beslutet.
	Rätten skall hålla förhandling

i saken så snart det kan ske och senast på fjärde dagen efter det att framställningen kom in till rätten.

28 kap.

1 a §

Om det finns anledning att anta att brott, på vilket fängelse kan följa, har förövats får, för ändamål som anges i 1 §, hos den som är skäligen misstänkt, husrannsakan företas i en dator, ett datorsystem eller annan liknande teknisk utrustning för att söka efter data i elektronisk form.

Husrannsakan enligt första stycket får företas hos annan, men endast om brottet har förövats hos honom eller den misstänkte har gripits där eller det annars finns synnerlig anledning att anta att det genom husrannsakan skall anträffas något som får tas i beslag eller att annan utredning om brottet skall vinnas. Som grund för en sådan husrannsakan får åberopas samtycke av den hos vilken åtgärden skall företas.

Om det finns särskilda skäl får husrannsakan verkställas via ett kommunikationsnät.

4 §[7]

Förordnande om husrannsakan meddelas, *utom i fall som avses i tredje stycket*, av undersökningsledaren eller rätten. Förordnande om husrannsakan för delgivning skall alltid meddelas av rätten. Kan i annat fall husrannsakan antas bli av stor omfattning eller medföra synnerlig olägenhet för den hos vilken åtgärden företas, bör, om det inte är fara i dröjsmål, åtgärden inte vistas utan rättens förordnande.	Förordnande om husrannsakan meddelas, *om inte annat är föreskrivet*, av undersökningsledaren eller rätten. *Beslut om husrannsakan enligt 1 a § tredje stycket meddelas av rätten, eller av åklagaren om det föreligger samtycke.* Förordnande om husrannsakan för delgivning skall alltid meddelas av rätten. Kan i annat fall husrannsakan antas bli av stor omfattning eller medföra synnerlig olägenhet för den hos vilken åtgärden företas, bör, om det inte är fara i dröjsmål, åtgärden inte vistas utan rättens förordnande.

Fråga om husrannsakan får rätten ta upp på yrkande av undersökningsledaren eller åklagaren. Efter åtalet får rätten även på yrkande av målsägande eller självmant ta upp en sådan fråga. Fråga om husrannsakan för delgivning tas upp av rätten självmant eller på yrkande av polismyndighet eller åklagaren.

Förordnande om husrannsakan för eftersökande av den som skall häktas enligt beslut som avses i 24 kap. 17 § tredje stycket eller hämtas till inställelse vid rätten meddelas av polismyndighet eller polisman enligt bestämmelser i polislagen.

[7] Senaste lydelse 1995:637.

	5 §[8]
En polisman får företa husrannsakan utan förordnande enligt 4 § om det är fara i dröjsmål. Detta gäller dock inte husrannsakan för delgivning.	En polisman får företa husrannsakan utan förordnande enligt 4 § om det är fara i dröjsmål. Detta gäller dock inte husrannsakan för delgivning *eller husrannsakan enligt 1 a §.*
	6 §
Vid husrannsakan *må* olägenhet eller skada *ej* förorsakas utöver vad som är oundgängligen nödvändigt. Rum eller förvaringsställe *må*, om det *erfordras*, öppnas med våld. *Har så* skett, skall det efter förrättningen på lämpligt sätt åter tillslutas. Husrannsakan *må ej* utan särskilt skäl verkställas mellan klockan nio eftermiddagen och klockan sex förmiddagen.	Vid husrannsakan *får* olägenhet eller skada *inte* förorsakas utöver vad som är oundgängligen nödvändigt. Rum eller förvaringsställe *får*, om det *behövs*, öppnas med våld. *Om så har* skett, skall det efter förrättningen på lämpligt sätt åter tillslutas. Husrannsakan *får inte* utan särskilt skäl verkställas mellan klockan nio *på* eftermiddagen och klockan sex *på* förmiddagen. *Vad som nu har sagts gäller inte husrannsakan enligt 1 a § tredje stycket.*
	7 §
Vid husrannsakan skall *såvitt* möjligt ett av förrättningsmannen anmodat trovärdigt vittne närvara. Förrättningsmannen *äge* anlita *erforderligt* biträde av sakkunnig eller annan.	Vid husrannsakan skall *om* möjligt ett av förrättningsmannen anmodat trovärdigt vittne närvara. Förrättningsmannen *får* anlita *nödvändigt* biträde av sakkunnig eller annan.

[8] Senaste lydelse 1995:637.

Den, hos vilken husrannsakan *företages*, eller, om han *ej* är *tillstädes*, *hans* hemmavarande *husfolk* skall *erhålla* tillfälle att *övervara* förrättningen *så ock* att tillkalla vittne, dock utan att undersökningen därigenom *uppehålles*. Har varken han eller någon *av hans husfolk* eller av dem tillkallat vittne *närvarit*, skall han, så snart det kan ske utan men för utredningen, underrättas om den vidtagna åtgärden.

Vid förrättningen *må* målsägande eller hans ombud tillåtas att närvara för att tillhandagå med *nödiga* upplysningar; *dock skall tillses*, att målsäganden eller ombudet *icke* i vidare mån än för ändamålet *erfordras vinner* kännedom om förhållande, som därvid *yppas*.

Den, hos vilken husrannsakan *företas*, eller, om han *inte* är *närvarande*, *annan* hemmavarande skall *ges* tillfälle att *närvara vid* förrättningen *samt* att tillkalla vittne, dock utan att undersökningen därigenom *uppehålls*. Har varken han eller någon *annan hemmavarande* eller *något* av dem tillkallat vittne *varit närvarande*, skall han, så snart det kan ske utan men för utredningen, underrättas om den vidtagna åtgärden.

Vid förrättningen *får en* målsägande eller hans ombud tillåtas att närvara för att tillhandagå med *nödvändiga* upplysningar. *Den som verkställer åtgärden skall tillse* att målsäganden eller ombudet *inte* i vidare mån än *vad som krävs* för ändamålet *får* kännedom om förhållande, som därvid *röjs*.

Första stycket första meningen, andra stycket första meningen och tredje stycket gäller inte vid husrannsakan enligt 1 a § tredje stycket.

38 kap.

2 §

Innehar någon skriftlig handling som kan *antagas äga*

Innehar någon skriftlig handling som kan *antas ha* be-

betydelse som bevis, *vare* han skyldig att förete den; sådan skyldighet *åligge* dock *ej* i brottmål den misstänkte eller den som till honom står i sådant förhållande, som avses i 36 kap. 3 §.

Ej vare part eller honom närstående, som nu sagts, skyldig att förete skriftligt meddelande mellan parten och någon honom närstående eller mellan sådana närstående inbördes. Befattningshavare eller annan, som avses i 36 kap. 5 §, *må ej* förete skriftlig handling, om dess innehåll kan *antagas* vara sådant, att han *ej må* höras som vittne därom; *innehaves* handlingen av part, till förmån för vilken tystnadsplikten gäller, *vare* han *ej* skyldig att förete handlingen. *Stadgandet* i 36 kap. 6 § om vittnes rätt att vägra yttra sig *äge* motsvarande *tillämpning* i fråga om innehavare av skriftlig handling, om dess innehåll är sådant, som avses i nämnda lagrum.

Skyldighet att förete handling *gälle ej* minnesanteckning eller annan sådan uppteckning, som är avsedd uteslutande för personligt bruk, *med mindre* synnerlig anledning *förekom-*

tydelse som bevis, *är* han skyldig att förete den. Sådan skyldighet *åligger* dock *inte* i brottmål den misstänkte eller den som till honom står i sådant förhållande, som avses i 36 kap. 3 §.

En part eller *någon* honom närstående, som nu *har* sagts, *är inte* skyldig att förete skriftligt meddelande mellan parten och någon honom närstående eller mellan sådana närstående inbördes. *En* befattningshavare eller annan, som avses i 36 kap. 5 §, *får inte* förete *en* skriftlig handling, om dess innehåll kan *antas* vara sådant, att han *inte får* höras som vittne därom; *innehas* handlingen av part, till förmån för vilken tystnadsplikten gäller, *är* han *inte* skyldig att förete handlingen. *Bestämmelsen* i 36 kap. 6 § om vittnes rätt att vägra yttra sig *skall tillämpas också* i fråga om innehavare av skriftlig handling, om dess innehåll är sådant, som avses i nämnda lagrum.

Skyldigheten att förete handling *gäller inte* minnesanteckning eller annan sådan uppteckning, som är avsedd uteslutande för personligt bruk, *om det inte finns* synnerlig an-

mer, att den företes.

ledning att den företes.

Bestämmelserna om skriftlig handling gäller även för elektronisk upptagning av skrift.

39 kap.

5 §[9]

Innehar någon föremål, som lämpligen kan flyttas till rätten och som kan *antagas äga* betydelse som bevis, *vare* han skyldig att tillhandahålla det för syn; sådan skyldighet *åligge* dock *ej* i brottmål den misstänkte eller den som till honom står i sådant förhållande, som avses i 36 kap. 3 §. *Stadgandet* i 36 kap. 6 § om vittnes rätt att vägra yttra sig *äge* motsvarande *tillämpning* i fråga om rätt för part eller annan att vägra tillhandahålla föremål för syn. Om skyldighet att förete skriftlig handling för syn gäller vad *i* 38 kap. 2 § *är stadgat*.

Vad *i* 38 kap. 3-9 §§ är *stadgat äge* motsvarande tillämpning beträffande föremål eller skriftlig handling som skall tillhandahållas.

Innehar någon föremål, som lämpligen kan flyttas till rätten och som kan *antas ha* betydelse som bevis, *är* han skyldig att tillhandahålla det för syn. Sådan skyldighet *åligger* dock *inte* i brottmål den misstänkte eller den som till honom står i sådant förhållande, som avses i 36 kap. 3 §. *Bestämmelsen* i 36 kap. 6 § om vittnes rätt att vägra yttra sig *skall tillämpas också* i fråga om rätt för part eller annan att vägra tillhandahålla föremål för syn. Om skyldighet att förete skriftlig handling *eller elektronisk upptagning av skrift* för syn gäller vad *som är föreskrivet i* 38 kap. 2 §.

Vad *som föreskrivs i* 38 kap. 3-9 §§ *skall tillämpas också* beträffande föremål eller skriftlig handling som skall tillhandahållas.

Denna lag träder i kraft den ……..

[9] Senaste lydelse 1980:101.

2.2 Förslag till lag om ändring i lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål

Härigenom föreskrivs i fråga om lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål
att 5 § skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 §[10]
Tillstånd enligt 27 kap. rättegångsbalken till hemlig teleavlyssning *eller* hemlig teleövervakning får meddelas, även om brottet inte omfattas av 27 kap. 18 eller 19 § rättegångsbalken. Tillstånd till hemlig kameraövervakning får meddelas enligt lagen (1995:1506) om hemlig kameraövervakning, även om brottet inte omfattas av 2 § i den lagen.	Tillstånd enligt 27 kap. rättegångsbalken till hemlig teleavlyssning, hemlig teleövervakning *eller frysning av elektronisk kommunikation* får meddelas, även om brottet inte omfattas av 27 kap. 18 eller 19 § rättegångsbalken. Tillstånd till hemlig kameraövervakning får meddelas enligt lagen (1995:1506) om hemlig kameraövervakning, även om brottet inte omfattas av 2 § i den lagen.
Kan det befaras att inhämtande av rättens tillstånd till *hemlig teleavlyssning, hemlig teleövervakning eller* hemlig kameraövervakning skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.	Kan det befaras att inhämtande av rättens tillstånd till hemlig kameraövervakning skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.

[10] Senaste lydelse 1995:1507.

Denna lag träder i kraft den ……..

2.3 Förslag till lag om ändring i brottsbalken (1962:700)

Härigenom föreskrivs i fråga om brottsbalken
dels att 4 kap. 9 c § och 14 kap. 9 § skall ha följande lydelse,
dels att det skall införas en paragraf, 4 kap. 9 d §, med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	9 c §[11]
Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för *automatisk* databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för ***dataintrång*** till böter eller fängelse i högst två år. Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för *automatisk databehandling*.	Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för *automatiserad* databehandling eller olovligen ändrar eller utplånar eller i register för in *en* sådan upptagning eller *med tekniskt hjälpmedel avlyssnar elektromagnetiska emissioner eller andra icke allmänt tillgängliga signaler till eller från en dator eller inom ett datorsystem i syfte att få del av information* döms för ***dataintrång*** till böter eller fängelse i högst två år. Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för *automatiserad informationsbehandling*.

[11] Senaste lydelse 1998:206. Här återges paragrafen utan de ändringar som har föreslagits i promemorian om genomförande av EU:s IT-rambeslut (Ds 2005:5). Beträffande dessa se kapitel 10.

9 d §

Om någon anbringar ett tekniskt hjälpmedel med uppsåt att föröva dataintrång bestående i avlyssning av elektromagnetiska emissioner eller andra icke allmänt tillgängliga signaler, döms för förberedelse till sådant brott till böter eller fängelse i högst två år, om han inte har gjort sig skyldig till fullbordat brott.

14 kap.

9 §

Den som åberopar falsk urkund, *utbjuder* eller håller till salu verk med falsk signatur, *utprånglar* falsk sedel eller falskt mynt, begagnar falskt värde- eller kontrollmärke, åberopar falskt fast märke eller *eljest* gör bruk av något som förfalskats på sätt som ovan sägs, *dömes*, om åtgärden innebär fara i bevishänseende, för brukande av det förfalskade *såsom hade han* själv gjort förfalskningen.

Den som åberopar falsk urkund, *bjuder ut* eller håller till salu verk med falsk signatur, *prånglar ut* falsk sedel eller falskt mynt, begagnar falskt värde- eller kontrollmärke, åberopar falskt fast märke eller *annars* gör bruk av något som förfalskats på sätt som ovan sägs, *döms*, om åtgärden innebär fara i bevishänseende, för brukande av det förfalskade *som om han* själv *hade* gjort förfalskningen.

För brukande av falsk urkund döms även den som åberopar en icke autentisk sammanställning av elektroniska data och därvid ger sken av att den är autentisk, om åtgärden innebär fara i bevishänseende.

---

1. Denna lag träder i kraft den……
2. I fråga om gärningar som har begåtts före ikraftträdandet gäller äldre bestämmelser.

2.4 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs i fråga om sekretesslagen (1980:100) att 16 kap. 1 § skall ha följande lydelse.

1 §[12]

Nuvarande lydelse

Att friheten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter i vissa fall är begränsad framgår av 7 kap. 3 § första stycket 1 och 2, 4 § 1-8 samt 5 § 1 och 3 tryckfrihetsförordningen och av 5 kap. 1 § första stycket samt 3 § första stycket 1 och 2 yttrandefrihetsgrundlagen. De fall av uppsåtligt åsidosättande av tystnadsplikt, i vilka nämnda frihet enligt 7 kap. 3 § första stycket 3 och 5 § 2 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 3 yttrandefrihetsgrundlagen i övrigt är begränsad, är de där tystnadsplikten följer av

---

3. denna lag enligt

---

5 kap. 1 §	såvitt avser uppgift om kvarhållande av försändelse *på befordringsföretag*, hemlig teleavlyssning *och* hemlig teleövervakning eller hemlig kameraövervakning på grund av beslut av domstol, undersökningsledare eller åklagare

5 kap. 2-4 §§

[12] Senaste lydelse 2004:509.

5 kap. 7 §	såvitt avser uppgift om kvarhållande av försändelse *på befordringsföretag*, hemlig teleavlyssning *och* hemlig teleövervakning eller hemlig kameraövervakning på grund av beslut av domstol, undersökningsledare eller åklagare

---

Föreslagen lydelse

Att friheten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter i vissa fall är begränsad framgår av 7 kap. 3 § första stycket 1 och 2, 4 § 1-8 samt 5 § 1 och 3 tryckfrihetsförordningen och av 5 kap. 1 § första stycket samt 3 § första stycket 1 och 2 yttrandefrihetsgrundlagen. De fall av uppsåtligt åsidosättande av tystnadsplikt, i vilka nämnda frihet enligt 7 kap. 3 § första stycket 3 och 5 § 2 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 3 yttrandefrihetsgrundlagen i övrigt är begränsad, är de där tystnadsplikten följer av

---

3. denna lag enligt

---

5 kap. 1 §	såvitt avser uppgift om kvarhållande av försändelse *enligt 27 kap. 9 eller 9 a § rättegångsbalken*, hemlig teleavlyssning, hemlig teleövervakning, *frysning av elektronisk kommunikation* eller hemlig kameraövervakning på grund av beslut av

	domstol, undersökningsledare eller åklagare
5 kap. 2-4 §§	
5 kap. 7 §	såvitt avser uppgift om kvarhållande av försändelse *enligt 27 kap. 9 eller 9 a § rättegångsbalken*, hemlig teleavlyssning, hemlig teleövervakning, *frysning av elektronisk kommunikation* eller hemlig kameraövervakning på grund av beslut av domstol, undersökningsledare eller åklagare
7 kap. 1 §	såvitt avser uppgift om annat än verkställigheten av beslut om omhändertagande eller beslut om vård utan samtycke

---

Denna lag träder i kraft den ……..

2.5 Förslag till lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Härigenom föreskrivs i fråga om lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.
att 28 § skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	28 §[13]
Kan det befaras att inhämtande av rättens tillstånd till *hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken*, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller hemlig kameraövervakning skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får åtgärden beslutas av åklagaren. I fråga om kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken får åtgärden även beslutas av undersökningsledaren. Anmälan som avses i *tredje stycket nämnda paragraf* skall göras hos den som har fattat beslutet. Denne skall pröva beslagsfrågan.	Kan det befaras att inhämtande av rättens tillstånd till kvarhållande av försändelse enligt 27 kap. 9 *eller 9 a* § rättegångsbalken eller hemlig kameraövervakning skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får åtgärden beslutas av åklagaren. I fråga om kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken får åtgärden även beslutas av undersökningsledaren. Anmälan som avses i *27 kap. 9 § tredje stycket och 9 a § tredje stycket* skall göras hos den som har fattat beslutet. Denne skall pröva beslagsfrågan.

[13] Senaste lydelse 1995:1509.

Om undersökningsledaren eller åklagaren har meddelat ett beslut med stöd av första stycket, skall det genast anmälas hos rätten. Anmälan skall vara skriftlig och innehålla skälen för beslutet. Rätten skall pröva ärendet snabbt. Anser rätten att beslutet inte bör bestå, skall det upphävas.	Om undersökningsledaren eller åklagaren har meddelat ett beslut med stöd av första stycket, skall det, *om inte annat föreskrivs i 27 kap. 21 a § rättegångsbalken*, genast anmälas hos rätten. Anmälan skall vara skriftlig och innehålla skälen för beslutet. Rätten skall pröva ärendet snabbt. Anser rätten att beslutet inte bör bestå, skall det upphävas.

Denna lag träder i kraft den……

2.6 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål

dels att 1 kap. 2 §, 2 kap. 1, 2 och 4 §§, 3 kap. 1 § samt 4 kap. 18, 20 och 25 §§ skall ha nedan angivna lydelse,

dels att det i lagen skall införas fem nya paragrafer, 4 kap. 26 a-d och 28 a §§, med följande lydelse,

dels att rubrikerna före 4 kap. 14 och 25 §§ skall ha följande lydelse,

dels att det före 4 kap 26 a och d §§ samt 28 a § skall införas tre nya rubriker med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	2 §[14]
Rättslig hjälp enligt denna lag omfattar följande åtgärder: 1. förhör i samband med förundersökning i brottmål, 2. bevisupptagning vid domstol, 3. telefonförhör, 4. förhör genom videokonferens, 5. kvarstad, beslag, samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,	Rättslig hjälp enligt denna lag omfattar följande åtgärder: 1. förhör i samband med förundersökning i brottmål, 2. bevisupptagning vid domstol, 3. telefonförhör, 4. förhör genom videokonferens, 5. kvarstad, beslag, *åtgärd enligt 27 kap. 15 § tredje stycket rättegångsbalken* samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken, *6. åtgärd enligt 27 kap. 9 och 9 a §§ rättegångsbalken,*

[14] Senaste lydelse 2003:1171. I Ds 2004:50 (se avsnitt 6.13.1) har också föreslagits ändring i paragrafen. Detta ändringsförslag har inte beaktats här.

6. hemlig teleavlyssning *och* hemlig teleövervakning,	*7.* hemlig teleavlyssning, hemlig teleövervakning *och frysning av elektronisk kommunikation*,
7. hemlig kameraövervakning,	*8.* hemlig kameraövervakning,
	9. röjande av trafikuppgifter,
8. överförande av frihetsberövade för förhör m.m., och	*10*. överförande av frihetsberövade för förhör m.m., och
9. rättsmedicinsk undersökning av en avliden person.	*11*. rättsmedicinsk undersökning av en avliden person.

Lagen hindrar inte att hjälp lämnas med annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

2 kap.

1 §[15]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1-*7* och 9 skall lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *1-9* och *11* skall lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.
Rättslig hjälp enligt 1 kap. 2 § första stycket *8* lämnas enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp enligt 1 kap. 2 § första stycket *10* lämnas enligt de särskilda bestämmelserna i denna lag.

[15] Senaste lydelse 2002:331. I Ds 2004:50 (se avsnitt 6.13.1) har också föreslagits ändring i paragrafen. Detta ändringsförslag har inte beaktats här.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §[16]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1-4 och *8* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5-*7* och 9 får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan *och* beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1-4 och *9-10* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5-*8* och *11* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, beslag *och åtgärd enligt 27 kap. 15 § tredje stycket rättegångsbalken*

4 §[17]

En ansökan om rättslig hjälp i Sverige enligt denna lag bör innehålla
- uppgift om den utländska domstol eller myndighet som handlägger ärendet,
- en beskrivning av det rättsliga förfarande som pågår,
- uppgift om den aktuella gärningen med tid och plats för denna, samt de bestämmelser som är tillämpliga i den ansökande staten,
- uppgift om vilken åtgärd som begärs och, i förekommande fall, i vilken egenskap en person skall höras,
- namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14 och 29 §§	I 4 kap. 8, 11, 14, *22 a, 28 a*

[16] Senaste lydelse 2002:331. I Ds 2004:50 (se avsnitt 6.13.1) har också föreslagits ändring i paragrafen. Detta ändringsförslag har inte beaktats här.
[17] I Ds 2004:50 (se avsnitt 6.13.1) har också föreslagits ändring i paragrafen. Detta ändringsförslag har inte beaktats här.

finns särskilda bestämmelser om vad en ansökan ytterligare skall innehålla vid vissa slag av åtgärder.

och 29 §§ finns särskilda bestämmelser om vad en ansökan ytterligare skall innehålla vid vissa slag av åtgärder.

En ansökan om rättslig hjälp skall göras skriftligen genom post, bud eller telefax. Den får även, efter överenskommelse i det enskilda fallet, översändas på annat sätt.

3 kap.

1 §[18]

Bestämmelserna i 2 kap. 4 § första och tredje styckena skall til??lämpas vid ansökan om rättslig hjälp utomlands, om inte annat följer av en internationell överenskommelse som är bindande för Sverige eller av krav från den mottagande staten.

I 4 kap. 9, 10 *och* 13 §§ finns särskilda bestämmelser om vad en ansökan *om telefonförhör och förhör genom videokonferens* skall innehålla.

I 4 kap. 9, 10, 13, *26 a-b och 28 a* §§ finns särskilda bestämmelser om vad en ansökan *ytterligare* skall innehålla *vid vissa slag av åtgärder*.

4 kap.

Kvarstad, beslag och husrannsakan samt vissa andra åtgärder som avses i 27 och 28 kap. rättegångsbalken m.m.

---

18 §

En ansökan om att andra åtgärder enligt 28 kap. rättegångsbalken än som avses i 16 § skall vidtas i Sverige handläggs av åklagare.

En ansökan om att andra åtgärder enligt *27 eller* 28 kap. rättegångsbalken än som avses i 16 § skall vidtas i Sverige handläggs av åklagare.

[18] I Ds 2004:50 (se avsnitt 6.13.1) har föreslagits en i sak motsvarande ändring i paragrafen.

20 §

Även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag, får husrannsakan enligt 16 § göras och egendomen tas i beslag och överlämnas till den ansökande staten om ansökan har gjorts av en stat som är medlem i Europeiska unionen eller av Norge eller Island och det för gärningen kan dömas till fängelse i den ansökande staten.	Även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag, får husrannsakan enligt 16 § göras och egendomen tas i beslag och överlämnas till den ansökande staten om ansökan har gjorts av en stat som är medlem i Europeiska unionen eller av Norge eller Island och det för gärningen kan dömas till fängelse i den ansökande staten. *Detsamma gäller en åtgärd enligt 27 kap. 15 § tredje stycket rättegångsbalken.*

I ett sådant ärende om rättslig hjälp som avses i 1 kap. 5 § första stycket 1 får husrannsakan göras samt egendom tas i beslag och överlämnas till den ansökande staten om den gärning ansökan avser motsvarar ett brott för vilket enligt svensk lag eller den ansökande statens lag är föreskrivet fängelse i sex månader eller mer. Vad som sagts nu gäller inte om första stycket är tillämpligt.

Hemlig teleavlyssning eller hemlig teleövervakning m.m.

Hemlig teleavlyssning och hemlig teleövervakning m.m. av någon i Sverige

25 §[19]

En ansökan om hemlig teleavlyssning eller hemlig teleövervakning av någon som befinner sig i Sverige handläggs av åklagare. Åklagaren skall genast pröva om det finns förutsättningar för

[19] I Ds 2004:50 (se avsnitt 6.13.1) har också föreslagits ändring i paragrafen. Detta ändringsförslag har inte beaktats här.

åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden.

Reglerna i 27 kap. 24 § rättegångsbalken skall inte tillämpas på upptagning eller uppteckning som gjorts vid hemlig teleavlyssning på begäran av en annan stat. Materialet får bevaras till dess att ärendet om rättslig hjälp har avslutats och återredovisning har skett enligt 2 kap. 17 §, om inte åklagaren dessförinnan med stöd av 26 b § har beslutat att materialet skall förstöras. Kvarvarande upptagningar eller uppteckningar som inte överlämnas till den andra staten skall därefter förstöras.

Frysning av elektronisk kommunikation m.m. i Sverige

26 a §[20]

En ansökan om frysning av elektronisk kommunikation skall innehålla uppgift om den teleadress som åtgärden skall avse eller andra uppgifter som kan bidra till att identifiera denna. Ansökan handläggs av åklagare. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden.

Beslutar åklagaren om frysning av elektronisk kommuni-

[20] I Ds 2004:50 har föreslagits att en ny paragraf med samma nummer men annat innehåll skall införas (se avsnitt 6.13.1). Detta förslag har inte beaktats här.

kation skall begäran om frysning behandlas som en ansökan om rättslig hjälp enligt 25 § första stycket. Beslutar rätten om hemlig teleavlyssning skall vad som sägs i 25 § andra stycket samt 26 b och c §§ tillämpas på materialet från avlyssningen.

26 b §[21]

En ansökan om frysning av elektronisk kommunikation skall inom sextio dagar följas av en begäran om att de uppgifter som har säkrats skall överlämnas. När ansökan har kommit in till åklagaren skall de uppgifter som har hämtats in bevaras till dess att denne tagit ställning till begäran. Om någon framställning inte görs inom den angivna tiden, eller om uppgifterna av annat skäl inte lämnas till den andra staten, skall de omedelbart förstöras.

Om ansökan om säkrande även innehåller en begäran om att få del av uppgifterna skall åklagaren utan hinder av vad som sägs i första stycket omedelbart pröva om dessa kan överlämnas.

[21] I Ds 2004:50 har föreslagits att en ny paragraf med samma nummer men annat innehåll skall införas (se avsnitt 6.13.1). Detta förslag har inte beaktats här.

26 c §[22]

Om det vid hemlig teleavlyssning, hemlig teleövervakning eller frysning av elektronisk kommunikation framkommer att en tjänsteleverantör i en tredje stat har medverkat i överföringen gäller samma skyldighet som föreskrivs i 28 a § andra stycket.

Frysning av elektronisk kommunikation i utlandet

26 d §[23]

Om frysning av elektronisk kommunikation eller annat säkrande av datalagrade uppgifter skall äga rum i en annan stat får åklagare ansöka om sådan rättslig hjälp om det har avtalats i en internationell överenskommelse eller om den anmodade staten annars ger sådan hjälp.

Säkrande och röjande av trafikuppgifter

28 a §

En ansökan om säkrande och röjande av lagrade trafikuppgifter skall innehålla uppgift som utpekar telemeddelandet. Ansökan, som skall handläggas av åklagare, skall prövas genast. I

[22] I Ds 2004:50 har föreslagits att en ny paragraf med samma nummer men annat innehåll skall införas (se avsnitt 6.13.1). Detta förslag har inte beaktats här.
[23] I Ds 2004:50 har föreslagits att en ny paragraf med samma nummer men annat innehåll skall införas (se avsnitt 6.13.1). Detta förslag har inte beaktats här.

fråga om säkrade uppgifter tillämpas 26 b §.

Finner åklagaren att en tjänsteleverantör i en tredje stat har medverkat i överföringen av meddelandet skall den ansökande staten omgående underrättas om detta och erhålla tillräcklig mängd trafikuppgifter för att tjänsteleverantören och den väg på vilken meddelandet har överförts skall kunna identifieras.

Denna lag träder i kraft den ……..

2.7 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation

att 6 kap. 1, 8, 19, 21och 22 §§ skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	1 §
I detta kapitel avses med	
elektroniskt meddelande: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som en del av sändningar av ljudradio- och TV-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om denna information inte kan sättas i samband med den enskilde abonnenten eller användaren av informationen,	
trafikuppgift: uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att faktureras detta meddelande.	
Begreppen handling, personuppgiftsansvarig och samtycke har i kapitlet samma innebörd som i personuppgiftslagen (1988:204).	
	Begreppet telemeddelande har i kapitlet samma innebörd som i 27 kap. 9 a § rättegångsbalken.
	8 §[24]
Bestämmelserna i 5-7 §§ gäller inte	Bestämmelserna i 5-7 §§ gäller inte
1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i	1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i

[24] I Ds 2004:50 har också föreslagits ändring av paragrafen (se avsnitt 6.13.1). Detta ändringsförslag har inte beaktats här.

5 § för att lösa tvister,	5 § för att lösa tvister,
2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning *eller* hemlig teleövervakning, eller	2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning, hemlig teleövervakning, *åtgärd enligt 27 kap. 9 a § rättegångsbalken eller frysning av elektronisk kommunikation* eller
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.
	19 §[25]
En verksamhet skall bedrivas så att beslut om hemlig teleavlyssning *och* hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av	En verksamhet skall bedrivas så att beslut om hemlig teleavlyssning, hemlig teleövervakning, *åtgärd enligt 27 kap. 9 a § rättegångsbalken och frysning av elektronisk kommunikation* kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av
1. ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till all-	1. ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till all-

[25] I SOU 2003:74 har också föreslagits ändring av paragrafen (se avsnitt 11.10.1).Detta ändringsförslag har inte beaktats här.

mänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller	mänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller
2. tjänster inom ett allmänt kommunikationsnät vilka består av	2. tjänster inom ett allmänt kommunikationsnät vilka består av
a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller	a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller
b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.	b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Innehållet i och uppgifter om avlyssnade och övervakade telemeddelanden skall göras tillgängliga så att informationen enkelt kan tas om hand.

Med telemeddelanden avses ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om frågor som avses i första och andra styckena samt får i enskilda fall medge undantag från kravet i första stycket.

21 §[26]

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till	Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till
1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken, eller	1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § *eller meddelanden enligt 27 kap. 9 a §* rättegångsbalken, eller
2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken.	2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken *eller*
	3. angelägenhet som avser frysning av elektronisk kommunikation enligt 27 kap. 21 a § rättegångsbalken.
	Uppgifter som har bevarats efter beslut om frysning av elektronisk kommunikation får lämnas ut efter beslut av domstol om hemlig teleavlyssning eller hemlig teleövervakning. I 22 § första stycket 4 finns bestämmelser om skyldigheten att lämna ut trafikuppgifter.

22 §[27]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till	Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till

[26] I Ds 2004:50 har också föreslagits ändring av paragrafen (se avsnitt 6.13.1). Detta ändringsförslag har inte beaktats här.
[27] Senaste lydelse 2003:743. I SOU 2003:74 har också föreslagits ändring av paragrafen (se avsnitt 11.10.1).Detta ändringsförslag har inte beaktats här.

uppgift som avses i 20 § första stycket skall på begäran lämna

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (1970:428), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brottet, om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,

3. uppgift som avses i 20 § första stycket 3 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,

uppgift som avses i 20 § första stycket skall på begäran lämna

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (1970:428), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brottet, om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,

3. uppgift som avses i 20 § första stycket 3 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, *dock inte uppgift som avses i 21 § andra stycket,*

4. uppgift som avses i 20 § första stycket 3 och som angår ett särskilt angivet meddelande till

	åklagarmyndighet eller polismyndighet, om det föreligger misstanke om brott och fängelse ett år kan följa på detta samt uppgiften behövs för att identifiera tjänsteleverantörerna och den väg som meddelandet har överförts,
4. uppgift som avses i 20 § första stycket 1 till en kronofogdemyndighet som behöver uppgiften i exekutiv verksamhet, om myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,	*5.* uppgift som avses i 20 § första stycket 1 till en kronofogdemyndighet som behöver uppgiften i exekutiv verksamhet, om myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,
5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende om kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),	*6.* uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende om kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),
6. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten skall kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),	*7.* uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten skall kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),
7. uppgift som avses i 20 §	*8.* uppgift som avses i 20 §

första stycket 1 till polismyndighet eller åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten skall kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och	första stycket 1 till polismyndighet eller åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten skall kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och
8. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.	*9.* uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.
Ersättning för att lämna ut uppgifter enligt första stycket *8* skall vara skälig med hänsyn till kostnaderna för utlämnandet.	Ersättning för att lämna ut uppgifter enligt första stycket *9* skall vara skälig med hänsyn till kostnaderna för utlämnandet.

Denna lag träder i kraft den .....

3 Bakgrund

Tillkomsten av Europarådets konvention om IT-relaterad brottslighet (Convention on Cybercrime ETS no.: 185) skall ses mot bakgrund av de djupgående förändringar i samhället som datoriseringen och de globala datornätverken har medfört. Användningen av Internet har fått ett enormt genomslag under senare år. Detta beror dels på att såväl myndigheter som företag i ökande utsträckning erbjuder tjänster via Internet, dels på att privatpersoner i allt större utsträckning har tillgång till Internet.

Internet har utan tvekan inneburit stora framsteg genom de nya möjligheterna att snabbt, enkelt och billigt ta del av, hämta in eller distribuera stora mängder information. Tillgängligheten till information av alla slag har ökat väsentligt. Samtidigt finns det nackdelar med de globala nätverken främst i form av anonymiteten och de snabba kommunikationsvägarna. Dessa kan bl.a. utnyttjas för att sprida information i brottsligt syfte, för att anonymt handla med förbjudna varor, för att begå informationsintrång eller för att hindra eller förstöra informationssystems drift eller för att åstadkomma annan skada. Teknikutvecklingen är således inte enbart av godo utan skapar också möjligheter att begå vissa brott utan att gärningsmannen vid något tillfälle befinner sig i det land där brottet äger rum. Eftersom det inte krävs någon fysisk närvaro har gärningsmannen större möjligheter än annars att dölja sin identitet. Brottsligheten kan också snabbt spridas över fler länder. Tekniken skapar vidare möjligheter att oberoende av gränserna utplåna bevisning om brottet samt att snabbt flytta ekonomiskt utbyte av brott från ett land till ett an-

nat. Allt detta försvårar givetvis både upptäckt och lagföring av brott.

Den ökande oron för att datorer och datornätverk skall användas för att begå brott, och svårigheterna att upptäcka och lagföra sådana brott, har skapat behov av en samordnad, effektiv kamp över gränserna mot brottslighet av detta slag.

I november 1996 beslutade därför Europarådets kommitté för brottsfrågor (CDPC) att uppdra åt en expertkommitté att utreda frågor rörande IT-relaterad brottslighet med sikte på en konvention eller annan bindande internationell överenskommelse. Efter beslut i ministerrådet påbörjades arbetet på en konvention om IT-relaterad brottslighet i april 1997. Den slutliga versionen av konventionen förelades ministerrådet i juni 2001. Konventionen antogs av ministerrådet den 8 november 2001. Till konventionen har utarbetats en förklarande rapport antagen samma dag. En preliminär översättning av konventionen har bifogats denna promemoria som *bilaga 1*.

Konventionen upprättades i Budapest den 23 november 2001 och undertecknades av Sverige samma dag.

Konventionen trädde i kraft den 1 juli 2004, då kravet på att fem stater (varav minst tre medlemsstater i Europarådet) hade ratificerat konventionen var uppfyllt.

4 Konventionens huvudsakliga innehåll

4.1 Den allmänna strukturen

Konventionen kan sägas ha tre huvudsyften. Det första är att åstadkomma en harmonisering av den nationella straffrätten beträffande brott som tas upp i konventionen. Det andra är att få fram nationella processrättsliga bestämmelser som tillgodoser behoven av regler för att på ett effektivt sätt utreda och lagföra IT-relaterade brott och andra brott som begår med hjälp av datorer samt för att ta tillvara bevisning i elektronisk form. Det tredje är att lägga grunden för ett effektivt internationellt samarbete.

Konventionen är indelad i fyra kapitel. Dessa innehåller definitioner (artikel 1), bestämmelser om åtgärder som skall vidtas på nationell nivå (artiklarna 2 – 13, som innehåller straffrättsliga regler, och artiklarna 14 – 22, som innehåller processrättsliga regler), bestämmelser om internationellt samarbete (artiklarna 23 – 35) och slutbestämmelser (artiklarna 36 – 48).

Konventionen är uppbyggd på samma sätt som andra internationella instrument som behandlar frågor av likartat slag. Det bör emellertid redan här nämnas att den del av konventionen som behandlar anpassningen av nationella processrättsliga regler inte har någon motsvarighet i andra fördrag av liknande slag. Möjligheterna att göra undantag från de processrättsliga reglerna är dessutom mycket begränsade.

I ingressen till konventionen framhålls behovet av balans mellan å ena sidan grundläggande mänskliga rättigheter, bl.a. yttrandefriheten och informationsfriheten. Utöver dessa inledande ut-

talanden behandlas inte frågor med anknytning till tryck- och yttrandefrihet i konventionen.

4.2 Definitioner

Konventionen inleds med att det i *artikel 1* anges innebörden av några viktiga termer.

Med *”datorsystem”* avses i konventionen en apparat eller grupp av apparater som är sammankopplade eller som hör samman med varandra, av vilka en eller flera genom ett program utför automatiserad behandling av uppgifter. Definitionen är avsedd att täcka såväl traditionella datorer som andra tekniska apparater som kan användas för datakommunikation, exempelvis moderna mobiltelefoner. Den omfattar både hårdvara och mjukvara och alla tekniska delar från hårddisk till skrivare. Definitionen omfattar såväl enstaka datorer som nätverk. Den täcker vidare alla typer av nätverk oavsett på vilket sätt de är tekniskt förbundna med varandra.

Definitionen av *”datorbehandlingsbara uppgifter”* bygger på Internationella standardiseringskommissionens (ISO) definition av begreppet. Med datorbehandlingsbara uppgifter avses framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett datorsystem. Definitionen omfattar även program. Däremot faller elektromagnetiska emissioner utanför definitionen. Definitionen avser data i elektronisk eller annat direkt processbar form.

Med *”tjänsteleverantör”* avses en offentlig eller privat enhet som erbjuder sina användare möjlighet att kommunicera med hjälp av datorsystem samt varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller användarna av en sådan tjänst. Det saknar betydelse om det är fråga om öppna eller slutna nätverk.

”Trafikuppgifter” är en form av hjälpmedel som skapas av datorerna själva i syfte att göra det möjligt att följa datakommunikationen från början till slutet. Med trafikuppgifter avses i konventionen varje typ av datorbehandlingsbara uppgifter som hän-

för sig till ett meddelande som förmedlas med hjälp av datorsystem och som genereras av ett datorsystem som ingick i kommunikationskedjan och som anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst (t.ex. elektronisk post).

Konventionen innehåller inget krav på att definitionerna skall införas i nationell rätt så länge det finns adekvata motsvarigheter där.

4.3 Straffrättsliga regler

4.3.1 Allmänt om bestämmelserna

Syftet med de straffrättsliga reglerna i konventionen är att förbättra möjligheterna att förhindra och förebygga IT-relaterade brott genom att skapa en gemensam minimistandard för sådana brott. Harmoniseringen av straffrätten har till syfte att förhindra bl.a. att brottsligheten flyttas från en stat till en annan med lindrigare lagstiftning och att underlätta internationellt samarbete såväl i fråga om utlämning som rättslig hjälp. Konventionen hindrar inte att den nationella rätten går längre i fråga om kriminalisering.

De straffrättsliga reglerna omfattar brott som är direkt riktade mot datorbehandlingbara uppgifter och datorsystem (artiklarna 2-6), datorrelaterade brott (artiklarna 7-8), innehållsrelaterade brott (artikel 9) och brott mot upphovsrätt m.m. (artikel 10). Konventionen behandlar enbart uppsåtliga brott.

I konventionen används genomgående uttrycket ”without right” i artiklarna om materiell straffrätt. Syftet med detta är att markera att ett visst förfarande, som formellt faller in under beskrivningen av vad som skall vara kriminaliserat, ändå kan vara tillåtet. Ett handlande kan exempelvis stödjas på medgivande eller avtal eller på omständigheter som enligt den nationella rätten utesluter straffrättsligt ansvar. Administrativa eller straffprocessuella ingripanden faller därför utanför, för att nämna några exempel. Hur uttrycket ”without right” skall tolkas måste be-

stämmas med utgångspunkt i det sammanhang där uttrycket förekommer och de principer som gäller i den nationella rätten. Uttrycket ”without right” har översatts med ”orättmätigt”.

4.3.2 Brott riktade mot datorsystem och datorbehandlingsbara uppgifter

Enligt *artikel 2* skall intrång i hela eller delar av datorsystem straffbeläggas. Som villkor för kriminalisering får uppställas krav på att brottet har begåtts genom intrång i säkerhetsåtgärder, med uppsåt att komma över datorbehandlingsbara uppgifter eller med annat brottsligt uppsåt eller att brottet har riktat sig mot ett datorsystem som är kopplat till ett annat datorsystem.

Olovlig avlyssning regleras i *artikel 3*. Parterna åläggs att kriminalisera avlyssning med tekniska hjälpmedel av dataöverföringar till, från eller inom ett datorsystem. En förutsättning är att överföringen inte är allmänt tillgänglig. Kriminaliseringen skall även omfatta elektromagnetiska emissioner. Som villkor för kriminalisering får uppställas krav på att brottet har begåtts med brottsligt uppsåt eller att brottet har riktat sig mot ett datorsystem som är sammankopplat med ett annat datorsystem.

I *artikel 4* behandlas datastörning som består i att någon skadar, raderar, försämrar, ändrar eller undertrycker datorbehandlingsbara uppgifter. Kriminaliseringen får inskränkas till brott som medför allvarlig skada.

Störning av datorsystem regleras i *artikel 5*. Parterna åläggs att kriminalisera gärningar som består i att någon allvarligt hindrar ett datorsystems drift genom att mata in, överföra, skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

Artikel 6 reglerar otillåtet bruk av sådant som kan användas som hjälpmedel vid brott. Kriminaliseringen skall omfatta att uppsåtligen, i syfte att främja något av brotten som omnämns i artiklarna 2-5, företa vissa åtgärder. De otillåtna åtgärderna är att tillverka, försälja, anskaffa för användning, importera, sprida eller att på annat göra tillgängliga

- en apparat, vari ingår ett program, som har skapats eller anpassats främst för att begå brott som nämns i artiklarna 2-5,
- ett datorlösenord, en åtkomstkod eller någon annan liknande uppgift som kan ge åtkomst till hela eller en del av ett datorsystem.

I termen göra tillgänglig ingår att lägga ut verktyg, som kan användas som hjälpmedel för brott, on line så att de blir allmänt tillgängliga. Termen avser också att täcka skapande och kompilering av hyperlänkar i avsikt att underlätta tillgången till sådana verktyg.

Vidare skall kriminaliseringen omfatta innehav av något av de uppräknade hjälpmedlen med uppsåt att det skall användas för att begå brott som anges i nyssnämnda artiklar. Det är tillåtet att för straffbarhet kräva att innehavet omfattar flera föremål.

Det framgår uttryckligen att artikeln inte skall tolkas så att straffansvar skall åläggas i de fall där gärningsmannen inte har haft till syfte att begå brott. Härigenom utesluts straffansvar exempelvis i de fall där föremålet är avsett för att testa eller skydda ett datorsystem.

Parterna får förbehålla sig rätten att inte införa straffbestämmelser så länge förbehållet inte gäller försäljning, spridning eller tillgängliggörande av lösenord, åtkomstkod eller liknande.

4.3.3 Datorrelaterade brott

I *artikel 7* behandlas datorrelaterad förfalskning. Kriminaliseringen skall omfatta brott som består i att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter så att resultatet blir icke autentiska uppgifter, om syftet är att dessa skall användas för rättsliga ändamål som om de vore autentiska. Det saknar betydelse om uppgifterna är i läsbar och förståelig eller annan form. Som villkor får uppställas krav på att det föreligger bedrägeriavsikt eller annat brottsligt uppsåt.

Datorrelaterat bedrägeri regleras i *artikel 8*. Kriminaliseringen skall omfatta att någon orsakar annan förlust av egendom genom att mata in, ändra, radera eller undertrycka datorbehandlingsbara

uppgifter eller genom att störa ett datorsystems drift. En förutsättning för straffansvar skall vara att handlandet äger rum i bedrägeriavsikt eller med annat brottsligt uppsåt att skaffa ekonomisk förmån åt sig själv eller någon annan.

4.3.4 Barnpornografibrott

Artikel 9 reglerar barnpornografibrott. De handlingar som skall kriminaliseras är följande
- att framställa barnpornografi i syfte att sprida den med hjälp av datorsystem,
- att bjuda ut eller tillgängliggöra barnpornografi med hjälp av datorsystem,
- att sprida eller överföra barnpornografi med hjälp av datorsystem,
- att anskaffa barnpornografi åt sig själv eller någon annan med hjälp av datorsystem och
- att inneha barnpornografi i ett datorsystem eller på ett medium för lagring av datainformation.

Med barnpornografi avses i konventionen pornografiskt material som visuellt avbildar
- en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd,
- en person som ser ut att vara minderårig som ägnar sig åt sådant handlande eller
- realistiska bilder som föreställer en minderårig som ägnar sig åt sådant handlande.

Med minderårig avses den som är under 18 år. En lägre åldersgräns får föreskrivas, dock inte lägre än 16 år.

En part kan förbehålla sig rätten att, helt eller delvis, avstå från kriminalisering av anskaffning och innehav av barnpornografi samt i fråga om s.k. föreställningspornografi.

4.3.5 Brott mot upphovsrätt m.m.

Brott mot upphovsrätt och närstående rättigheter behandlas i *artikel 10*. Vad som skall vara kriminaliserat är sådana intrång i upphovsrätt och närstående rättigheter som följer av förpliktelserna i vissa internationella överenskommelser, nämligen
- Paris-beslutet om revidering av Bernkonventionen för skydd för upphovsrätten till litterära och konstnärliga verk,
- Avtalet om handelsrelaterade aspekter av immaterialrätten,
- WIPO-fördraget om upphovsrätt,
- Romkonventionen om skydd för utövande konstnärer, framställare av fonogram och radioföretag samt
- WIPO-fördraget om framföranden och fonogram.

En grundläggande förutsättning är att brotten begås i kommersiell skala och med hjälp av datorsystem. Ideella rättigheter har undantagits från tillämpningsområdet. Konventionen ger parterna rätt att i begränsad utsträckning avstå från att införa straffrättsliga sanktioner, under förutsättning att andra effektiva motmedel finns och att dessa inte avviker från partens internationella förpliktelser enligt de nämnda överenskommelserna.

4.3.6 Medhjälp och försök

I *artikel 11* regleras försök och olika former av medhjälp till brott. Kriminaliseringen skall omfatta uppsåtlig medhjälp till brott enligt artiklarna 2–10. Det direkta syftet med medhjälpsgärningen skall vara att ett sådant brott skall begås.

Vidare skall kriminaliseringen omfatta uppsåtliga försök till brott enligt artiklarna 3–5, 7, 8 och 9.1 a och c. Parterna får förbehålla sig rätten att helt eller delvis inte införa ansvar för försöksbrott.

4.3.7 Juridiska personers ansvar

Ansvar för juridiska personer regleras i *artikel 12*. Juridiska personer skall kunna hållas ansvariga för sådana brott som straffbeläggs enligt konventionen, om brottet har begåtts till förmån för den juridiska personen av en fysisk person som antingen agerat självständigt eller som en del av den juridiska personens organisation. Dessutom krävs det att den fysiska personen har en ledande ställning inom den juridiska personen, grundad på vissa i artikeln angivna omständigheter.

Vidare skall en juridisk person kunna åläggas ansvar om ett brott som behandlas i konventionen har kunnat begås till följd av att någon i ledande ställning har försummat sin tillsyn eller kontroll.

Ansvaret för juridiska personer kan vara såväl straffrättsligt som civilrättsligt eller administrativt. Det får inte påverka straffansvaret för de fysiska personer som har begått brott.

4.3.8 Påföljder

Enligt *artikel 13* skall brotten i artiklarna 2–11 bestraffas med effektiva, proportionella och avskräckande påföljder. Vidare skall de juridiska personer som kan ställas till ansvar enligt artikel 12 på motsvarande sätt bli föremål för effektiva, proportionella och avskräckande brottspåföljder eller andra sanktioner.

4.4 Processrättsliga regler

4.4.1 Allmänt om bestämmelserna

De processrättsliga reglerna är indelade i avsnitt med utgångspunkt i typen av åtgärd. Avdelningen inleds med allmänna bestämmelser (artiklarna 14-15), som är gemensamma för hela det processrättsliga avsnittet. Härefter följer ett avsnitt om skyndsamt säkrande av lagrade uppgifter (artiklarna 16-17), skyldighet

att lämna uppgifter (artikel 18), husrannsakan och beslag (artikel 19) samt insamling i realtid av uppgifter (artiklarna 20 och 21).

I *artikel 14* anges tillämpningsområdet för de processrättsliga reglerna i konventionen. Syftet är att dessa, med undantag för artikel 21, skall tillämpas inte bara på brott enligt artiklarna 2-11 utan även på andra brott som har begåtts med hjälp av datorsystem samt på insamling av bevis som har elektronisk form. Tillämpningsområdet är således betydligt vidare än enbart de brott som konventionen tar upp. Vad som avses med uttrycket ”andra brott som begåtts med hjälp av datorsystem” definieras inte. Regleringen tar sikte på såväl lagrad datainformation som information som skapas i anslutning till datorkommunikation. Det finns inget som hindrar en stat att vidta andra tvångsåtgärder än de som anges i konventionen, så länge man uppnår ett motsvarande resultat (jfr artikel 39).

Rättssäkerhetsgarantier och andra villkor behandlas i *artikel 15*. Vid införandet, genomförandet och tillämpningen av de processrättsliga reglerna gäller de villkor och garantier som föreskrivs i den nationella rätten. Reglerna skall ge ett tillfredsställande skydd för mänskliga rättigheter och friheter, bl.a. de fri- och rättigheter som behandlas i den europeiska konventionen om de mänskliga rättigheterna och de grundläggande friheterna och i FN-konventionen om medborgerliga och politiska rättigheter. Rättssäkerhetsgarantierna skall, när så är lämpligt, bl.a. innefatta rättslig och annan oberoende tillsyn samt att ändamålet med åtgärderna och begränsningar i och varaktigheten av dessa är angivna.

4.4.2 Säkringsåtgärder m.m.

I *artikel 16* regleras hur lagrade datorbehandlingsbara uppgifter, som löper särskild risk att gå förlorade eller förändras, skall säkras. Konventionen kräver lagstiftning eller andra metoder som gör det möjligt att förelägga personer att bevara eller på annat liknande sätt åstadkomma skyndsamt säkrande av specificerade datorbehandlingsbara uppgifter, däribland trafikuppgifter. Det

skall vara möjligt att ålägga en person att bevara informationen så länge som det behövs (dock högst nittio dagar), för att möjliggöra för myndigheterna att förordna om utlämnande. Vidare skall det finnas möjlighet att ålägga personen att hemlighålla åtgärden.

Enligt a*rtikel 17* skall, i fråga om trafikuppgifter som skall bevaras enligt artikel 16, det genom lagstiftning eller andra metoder säkerställas att sådana trafikuppgifter är åtkomliga, oberoende av om en eller flera tjänsteleverantörer har varit engagerade i överföringen av meddelandet. Vidare skall regleringen medge att tillräcklig mängd trafikuppgifter snabbt röjs för myndigheterna, i syfte att den som tillhandahållit tjänsten och den väg som meddelandet har följt skall kunna identifieras.

Enligt *artikel 18* skall parterna införa lagstiftning eller andra metoder som gör det möjligt för behörig myndighet att beordra
- en person att lämna ut särskilt angivna datorbehandlingsbara uppgifter, som personen har i sin besittning eller har kontroll över, om dessa är lagrade i ett datorsystem eller i ett medium för lagring av datainformation och
- en tjänsteleverantör att lämna ut abonnentuppgifter.

Med abonnentuppgifter avses varje form av information som finns hos en tjänsteleverantör om dennes abonnenter som avser annat än trafikuppgifter eller innehållet i meddelanden. Det saknar betydelse om informationen består av datorbehandlingsbara uppgifter eller har annan form. Informationen skall vara av det slaget att det med dess hjälp kan utrönas bl.a. abonnentens identitet, postadress eller geografiska adress samt telefon- och annat accessnummer. Information om typ av kommunikationstjänst, fakturering, betalning och annan tillgänglig information samt uppgifter om var kommunikationsutrustningen finns omfattas också.

I *artikel 19* regleras husrannsakan och beslag av lagrad information. Parterna skall ha regler som ger behörig myndighet rätt att genom husrannsakan eller på annat sätt skaffa sig åtkomst till datorsystem eller delar av ett system inom partens territorium och den information som är lagrad där. Motsvarande gäller me-

dium för lagring av datainformation. Det skall också finnas möjlighet att omedelbart utvidga husrannsakan till andra datorsystem, om det finns anledning att tro att den information som eftersöks finns i andra system inom territoriet. Vidare skall det finnas möjlighet att säkra den information som blir tillgänglig. Reglerna skall göra det möjligt att ta i beslag eller på annat sätt säkra ett datorsystem eller delar av det eller ett medium för lagring av datorbehandlingsbara uppgifter, att kopiera uppgifterna och behålla en kopia, att bevara uppgifterna i oförändrad form samt att ta bort eller göra uppgifterna oåtkomliga. Vidare skall behörig myndighet, i den mån det är skäligt, kunna förelägga en person som har kunskap om ett visst datorsystem och dess säkerhetsfunktioner att lämna upplysningar om detta för att möjliggöra säkringsåtgärder.

I *artikel 20* regleras insamling av trafikuppgifter i realtid. Parterna skall ha regler som gör det möjligt för behörig myndighet att antingen samla in eller med tekniska hjälpmedel ta upp eller ålägga en tjänsteleverantör att samla in eller ta upp vissa trafikuppgifter i realtid eller att samarbeta med behörig myndighet i dess insamlande av sådana uppgifter.

De trafikuppgifter som avses är uppgifter om särskilt angivna meddelanden inom territoriet vilka överförs med hjälp av datorsystem. Skyldigheten begränsas av de tekniska möjligheterna att få fram uppgifterna.

En tjänsteleverantör skall kunna åläggas att hemlighålla verkställigheten av åtgärder som anges i artikeln och information som har samband därmed.

Artikel 21 reglerar avlyssning av innehållet i meddelanden. Parterna åtar sig att i fråga om vissa allvarliga brott, som bestäms i den nationella lagstiftningen, kunna avlyssna i realtid eller spela in innehållet i särskilt angivna meddelanden, som överförs med hjälp av datorsystem. Detta kan ske antingen genom att behörig myndighet samlar in eller tar upp meddelandena eller genom att den ålägger en tjänsteleverantör att inom ramen för existerande teknisk förmåga samla in eller ta upp sådana meddelanden.

Parterna skall kunna ålägga tjänsteleverantören att hemlighålla verkställigheten av åtgärder som anges i artikeln och information som har samband därmed.

4.5 Domsrätt

Regler om domsrätt finns i *artikel 22*. Parterna åtar sig att ha regler om domsrätt som omfattar brott mot artiklarna 2–11 begångna inom deras territorium, ombord på fartyg och luftfartyg som är hemmahörande hos parten eller av en av dess medborgare, om brottet är straffbart där det begicks eller om brottet inte faller under någon parts territoriella behörighet.

Parterna har rätt att, helt eller delvis, reservera sig mot reglerna om domsrätt utom såvitt gäller brott inom det egna territoriet.

Parterna åtar sig också att vidta åtgärder för att fastställa sin domsrätt i de fall där en påstådd gärningsman befinner sig inom partens territorium och denna har vägrat lämna ut personen i fråga enbart på grund av dennes nationalitet.

Konventionen utesluter inte att staterna har mera långtgående regler om domsrätt.

Om flera stater anser sig ha domsrätt i fråga om brott enligt konventionen skall de samråda om lämpligaste jurisdiktion.

4.6 Internationellt samarbete

4.6.1 Allmänt om bestämmelserna

Avdelningen som reglerar internationellt samarbete utgör en betydande del av konventionen. Den innehåller en allmän del där de grundläggande principerna läggs fast (artiklarna 23 – 28) och en del med särskilda bestämmelser om vissa tvångsåtgärder m.m. (artiklarna 29 – 35). Artiklarna om internationellt samarbete har, om inte annat anges, ett vidare tillämpningsområde än enbart de brott som anges i artiklarna 2-11, nämligen i fråga om utredning

och lagföring av alla typer av datorrelaterade brott och brott som har begåtts med hjälp av datorsystem samt insamling av bevis i elektronisk form om brott.

I *artikel 23* läggs de allmänna principerna för det internationella samarbetet fast. Med utgångspunkt i konventionen, internationella överenskommelser om rättsligt samarbete och andra överenskommelser samt den nationella lagstiftningen skall parterna i största möjliga utsträckning samarbeta med varandra för att utreda eller lagföra brott som nyss har nämnts eller för att samla in bevis i elektronisk form om brott.

4.6.2 Utlämning

Utlämning behandlas i *artikel 24*. Artikeln reglerar endast utlämning i de fall där det inte finns ett utlämningsavstal mellan parterna eller om parterna, trots att det finns ett sådant avtal, väljer att helt eller delvis använda bestämmelserna i artikeln i stället.

I konventionen regleras enbart utlämning för brott som anges i artiklarna 2-11. Brotten skall i båda staterna kunna bestraffas med ett års frihetsberövande (om det inte finns ett avtal som föreskriver lägre straff; då gäller detta). Parterna åtar sig att se till att brotten i konventionen är utlämningsbara om de träffar utlämningsavtal. Parter som kräver utlämningsavtal för utlämning kan använda konventionen som rättslig grund för utlämning.

I fråga om utlämning skall villkoren enligt lagen i den stat från vilken utlämning begärs eller tillämpliga utlämningsavtal gälla. Detta gäller även skälen för att vägra utlämning.

Om utlämning för brott enligt artiklarna 2-11 vägras enbart på grund av den sökta personens nationalitet eller därför att den part från vilken utlämning begärs anser sig ha domsrätt över brottet åtar sig denna att, efter framställning från den part som begärt utlämning, överlämna ärendet till behörig myndighet för lagföring samt att rapportera slutresultatet till den andra parten. Förundersökning och åtal skall följa samma regler som ett jämförbart brott i den lagförande staten.

4.6.3 Rättslig hjälp

De allmänna principerna för rättslig hjälp behandlas i *artikel 25*. Parterna skall i största möjliga utsträckning ge varandra hjälp för att utreda och lagföra brott som är IT-relaterade samt för insamling av bevis i elektronisk form om brott. Artikeln innehåller också detaljregler om kommunikationen mellan parterna.

Om det inte finns avvikande bestämmelser i någon annan artikel i den del av konventionen som reglerar internationellt samarbete skall den rättsliga hjälpen ges enligt de regler som gäller i den anmodade partens lagstiftning eller i tillämpliga avtal. Detta gäller även i fråga om vilka omständigheter som får läggas till grund för en vägran att ge rättslig hjälp. Den anmodade parten får inte vägra rättslig hjälp beträffande brott som anges i artiklarna 2-11 enbart på den grunden att det är fråga om ett brott som den betraktar som fiskalt.

I de fall där den anmodade parten har rätt att kräva dubbel straffbarhet för att lämna rättslig hjälp, skall det villkoret anses uppfyllt oberoende av hur brottet rubriceras i den nationella lagstiftningen, så länge handlandet är kriminaliserat.

I *artikel 26* regleras spontant uppgiftslämnande. En part kan, inom ramen för sin nationella lagstiftning, utan föregående framställning till en annan part lämna bl.a. uppgifter rörande brott som omfattas av konventionen. Den som spontant lämnar information kan, innan det sker, begära att uppgifterna hemlighålls eller ställa villkor för användningen av den. Om den mottagande parten inte är beredd att iaktta sådana begränsningar avgör den förstnämnda parten om informationen trots detta skall lämnas. Om mottagaren accepterar begränsningarna är detta bindande.

Artiklarna 27 och 28 behandlar förfarandet vid framställning om rättslig hjälp när det saknas tillämpliga internationella avtal. Även om det finns ett sådant avtal kan parterna enas om att artikel 27 helt eller delvis skall tillämpas.

Enligt *artikel 27* skall parterna peka ut en eller flera centrala myndigheter som skall ansvara för att sända och ta emot framställningar om rättslig hjälp, verkställa sådana framställningar

eller lämna över framställningarna till rätt myndighet. Centralmyndigheterna skall kommunicera direkt med varandra.

Rättslig hjälp skall ges i enlighet med det förfarande som anges av den begärande parten, om inte detta strider mot den anmodade partens lagstiftning. En anmodad part får, utöver vad som anges i artikel 25 punkt 4, avslå en framställning om rättslig hjälp om framställningen rör ett brott som betraktas som ett politiskt brott eller ett brott som har anknytning till ett politiskt brott eller om verkställandet av framställningen kan komma att inkräkta på partens suveränitet, säkerhet, allmänna rättsprinciper eller andra väsentliga intressen.

Den anmodade parten får skjuta upp verkställigheten av en begäran om rättslig hjälp om det skulle störa förundersökningar eller rättegångar som bedrivs av dess myndigheter. Ett avslag eller uppskjutande skall föregås av samråd och överväganden om framställningen kan bifallas till viss del eller under vissa villkor.

Den begärande parten skall så snart som möjligt informeras om resultatet av framställningen. Beslut om avslag eller om att skjuta upp verkställigheten skall innehålla skälen för beslutet. Den begärande parten skall vidare informeras om skäl som gör att framställningen kan komma att avslås eller försenas väsentligt.

Den begärande parten kan kräva att en framställning om rättslig hjälp hemlighålls, med undantag för vad som krävs för att verkställa den rättsliga hjälpen. Om den anmodade parten inte kan tillmötesgå ett sådant krav skall den omgående underrätta den andra parten om detta, varvid denna skall överväga om framställningen ändå skall fullföljas.

Artikeln innehåller också bestämmelser om kommunikationen mellan parterna.

I *artikel 28* finns bestämmelser om sekretess och användningsbegränsning som är avsedda att tillämpas när det inte finns något avtal om rättslig hjälp mellan parterna. Om parterna enas om det kan artikeln, eller delar av den, tillämpas även om det finns en bindande överenskommelse mellan dem.

I *artikel 29* regleras skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter. Syftet är att förhindra att uppgifterna går förlorade. En part får anmoda en annan part att genom föreläggande eller på annat sätt skyndsamt säkra uppgifter som lagrats med hjälp av ett datorsystem inom dennas territorium och vilka den begärande parten avser att begära åtkomst till genom rättslig hjälp med husrannsakan, beslag eller annan motsvarande åtgärd eller med röjande av uppgifterna. I artikeln anges närmare vilka uppgifter som en sådan framställning skall innehålla.

Säkrandet skall gälla under en period om minst sextio dagar, för att göra det möjligt för den begärande parten att överlämna en framställning om rättslig hjälp med husrannsakan, beslag eller annan liknande åtgärd eller med röjande av uppgifterna. När en sådan framställning mottagits skall uppgifterna bevaras till dess att ställning har tagits till framställningen.

Om det, vid verkställandet av rättslig hjälp med att säkra trafikuppgifter enligt artikel 29, upptäcks att en tjänsteleverantör i en annan stat har medverkat i överföringen av ett särskilt angivet meddelande, skall den anmodade parten enligt *artikel 30* skyndsamt för den begärande parten röja en tillräcklig mängd trafikuppgifter för att tjänsteleverantören i fråga och den väg som meddelandet har överförts skall kunna identifieras. Röjande av trafikuppgifter får vägras endast under samma förutsättningar som säkrande enligt artikel 29 får vägras.

Artiklarna 31-34 behandlar ömsesidig hjälp avseende utredningsbefogenheter. Enligt a*rtikel 31* får en part begära rättslig hjälp med husrannsakan, beslag eller andra liknande åtgärder i syfte att säkra och röja uppgifter som lagrats med hjälp av ett datorsystem i den anmodade parten, bl.a. uppgifter som har säkrats enligt artikel 29. Framställningen skall besvaras skyndsamt när det finns skäl att tro att uppgifterna löper särskild risk att gå förlorade eller förändras eller när den nationella lagstiftningen, konventionen eller andra internationella överenskommelser föreskriver skyndsamt samarbete.

Åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga eller som är åtkomliga med stöd av samtycke

behandlas i *artikel 32*. En part har rätt att, utan rättslig hjälp, skaffa sig tillgång till sådan lagrad information som är allmänt tillgänglig, oavsett var denna finns rent geografiskt. På motsvarande sätt skall en part, via ett datorsystem inom det egna territoriet, kunna skaffa sig åtkomst till eller ta emot sådana lagrade datorbehandlingsbara uppgifter som finns hos en annan part, om det sker med stöd av ett lagenligt och frivilligt samtycke av en person som har rätt att röja uppgifterna.

Artikel 33 behandlar rättslig hjälp med insamling av trafikuppgifter. Parterna skall lämna rättslig hjälp med insamling i realtid av trafikuppgifter rörande sådana särskilt angivna meddelanden som överförs med hjälp av datorsystem inom partens territorium. Hjälpen skall följa de villkor och former som gäller för den nationella rätten. Rättslig hjälp skall dock åtminstone omfatta sådana brott för vilka trafikuppgifter skulle kunna samlas in i realtid i ett motsvarande nationellt förfarande.

I *artikel 34* behandlas hjälp i form av hemlig teleavlyssning. Parterna åtar sig att, så långt den nationella lagstiftningen och tillämpliga överenskommelser medger det, tillhandahålla rättslig hjälp i form av hemlig teleavlyssning i realtid beträffande särskilt angivna meddelanden.

Enligt *artikel 35* skall parterna peka ut en nationell kontaktpunkt, som kan nås dygnet runt alla dagar i veckan, för att säkerställa omedelbar hjälp i frågor som rör IT-relaterade brott samt för insamling av bevisning i elektronisk form i brottmål. Om kontaktpunkten inte tillhör en myndighet som själv är behörig att handlägga frågor om rättslig hjälp och utlämning skall den omedelbart kunna hänvända sig till behörig myndighet.

4.7 Slutbestämmelser

I *artikel 36* regleras vilka som kan underteckna konventionen, hur detta kan ske och när konventionen träder i kraft. Såväl medlemmar av Europarådet som andra stater som har deltagit i utformningen av konventionen kan ansluta sig till denna.

Möjligheten att ansluta sig till konventionen sedan denna har trätt i kraft regleras i *artikel 37*. Artikeln öppnar en möjlighet att låta stater som varken är medlemmar av Europarådet eller som har deltagit i utformningen av konventionen ansluta sig.

I samband med att en part binder sig för konventionen har den möjlighet att specificera för vilket eller vilka territorier som konventionen skall gälla. Detta, liksom rätten att senare utöka eller minska den territoriella tillämpningen, regleras i *artikel 38*.

Artikel 39 behandlar verkan av konventionen. Syftet med konventionen är att komplettera gällande multilaterala eller bilaterala överenskommelser mellan parterna, däribland reglerna i

- den europeiska utlämningskonventionen den 13 december 1957 (utlämningskonventionen; prop. 1958:139, SÖ 1959:65 och 1967:46),
- den europeiska konventionen om inbördes rättshjälp i brottmål den 20 april 1959 (prop. 1961:48, SÖ 1968:15) och
- tilläggsprotokollet till den europeiska konventionen om inbördes rättshjälp i brottmål den 17 mars 1978 (prop. 1978/79:80, SÖ 1979:12).

Sverige har tillträtt de aktuella konventionerna.

Om två eller flera parter redan tidigare har träffat överenskommelse eller bindande avtal rörande frågor som behandlas i konventionen eller på annat sätt har utvecklat en praxis på sådana områden får de reglera sina inbördes förhållanden med hänsyn härtill. Om emellertid parterna reglerar sina relationer i något avseende som behandlas i konventionen på annat sätt än som anges i denna får tillämpningen inte vara oförenlig med konventionens syften och principer. Det nordiska samarbetet kan ses som ett exempel på ett mera ingående samarbete i vissa avseenden. Detta torde stå i god överensstämmelse med konventionen.

I *artikel 40* anges uttömmande i vilken utsträckning en part kan utnyttja rätten att uppställa ytterligare rekvisit.

Artikel 41, som behandlar federala stater, saknar intresse för svenskt vidkommande.

Artikel 42 behandlar uttömmande rätten för parter att göra förbehåll.

Enligt *artikel 43* kan ett förbehåll enligt artikel 42 återtas helt eller delvis. Parterna förutsätts göra detta så snart omständigheterna medger det.

Frågan om hur förslag till ändringar i konventionen väcks och hur en sådan fråga skall behandlas regleras i *artikel 44*.

Hur tvister angående tolkningen av konventionen skall lösas anges i *artikel 45*. I första hand skall en lösning genom förhandling eller annat liknande medel väljas. Möjligheter som anvisas är att hänskjuta tvisten till CDPC, till skiljedom eller till Internationella domstolen.

I *artikel 46* regleras frågan om samråd med anledning av genomförande och tillämpning av konventionen, utbyte av information om viktiga rättsliga, politiska eller tekniska utvecklingsrön angående IT-relaterad brottslighet och om insamling av bevis i elektronisk form. Vidare läggs CDPC:s roll som stödjande organ fast. CDCP skall, senast tre år efter det att konventionen har trätt i kraft,[28] i samråd med parterna genomföra en översyn av samtliga bestämmelser och, om så krävs, föreslå ändringar.

Möjligheten till uppsägning av konventionen regleras i *artikel 47*. Varje part har rätt att när som helst säga upp konventionen. *Artikel 48* reglerar slutligen Europarådets generalsekreterares skyldighet att hålla parterna underrättade om undertecknanden, depositionsinstrument, ikraftträdande, förklaringar och förbehåll samt andra handlingar som rör konventionen.

[28] Dvs. senast år 2007.

5 Tilläggsprotokollet till konventionen

5.1 Bakgrunden

Under arbetet med konventionen om IT-relaterad brottslighet fanns det några frågor som inte hann slutbehandlas. Dessa har tagits upp i ett tilläggsprotokoll till konventionen.

Tilläggsprotokollet behandlar kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem. Syftena med protokollet är två. Det ena är att åstadkomma en harmonisering av den materiella straffrätten i fråga om rasistiska och främlingsfientliga gärningar. Det andra är att förbättra det internationella samarbetet vid bekämpning av sådana brott.

Tilläggsprotokollet upprättades i Strasbourg den 28 januari 2003 (ETS no 189). Det undertecknades av Sverige samma dag.

Till protokollet har utarbetats en förklarande rapport antagen av ministerrådet den 7 november 2002.

En preliminär översättning av tilläggsprotokollet har fogats till denna promemoria som *bilaga 2.*

Tilläggsprotokollet har ännu inte trätt i kraft eftersom det inte har ratificerats av tillräckligt många stater.

5.2 Tilläggsprotokollets huvudsakliga innehåll

5.2.1 Den allmänna strukturen

Tilläggsprotokollet är indelat i fyra avdelningar. Den första avdelningen (artiklarna 1-2) innehåller gemensamma bestämmel-

ser. Den andra avdelningen (artiklarna 3-7) behandlar åtgärder som skall vidtas på nationell nivå. Den tredje avdelningen (artikel 8) tar upp förhållandet mellan konventionen och tilläggsprotokollet och den fjärde (artiklarna 9-16) innehåller slutbestämmelser.

5.2.2 Inledande bestämmelser m.m.

I ingressen till protokollet uttrycks oro för risken för att datorsystem kan missbrukas för att sprida rasistisk och främlingsfientlig propaganda. Det framhålls att gärningar av rasistisk och främlingsfientlig natur utgör en kränkning av de mänskliga rättigheterna och ett hot mot rättssamhället. Samtidigt erkänns att yttrandefriheten utgör en av de viktigaste grundvalarna i ett demokratiskt samhälle och en grundläggande förutsättning för samhällets framåtskridande och varje människas utveckling. Vidare betonas behovet av att säkerställa en lämplig avvägning mellan yttrandefriheten och bekämpning av gärningar av rasistisk eller främlingsfientlig natur. Det framhålls också att tilläggsprotokollet inte avser att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem.

I *artikel 1* anges syftet med tilläggsprotokollet, som är att komplettera bestämmelserna i konventionen om IT-relaterad brottslighet i fråga om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som begås med hjälp av datorsystem.

Artikel 2 innehåller en definition av rasistiskt och främlingsfientligt material. Med detta avses i protokollet skrivet material, bild eller annan framställning av idéer eller teorier som förespråkar, främjar eller uppmuntrar till hat, diskriminering eller våld mot en enskild person eller en grupp av personer på grund av ras, hudfärg, härstamning, nationellt eller etniskt ursprung eller trosbekännelse, om detta kännetecken tas som förevändning. Vidare slås det fast att de uttryck och termer som används i protokollet skall tolkas på samma sätt som de tolkas i konventionen.

5.2.3 Straffrättsliga regler

I likhet med konventionen behandlar protokollet enbart uppsåtliga gärningar. Dessa skall vidare ha begåtts ”without right”, vilket är samma uttryck som används i konventionen (se avsnitt 2.3.1). I motsats till vad som är fallet med de gärningar som behandlas i konventionen ställs det inga krav på att de gärningar som behandlas i tilläggsprotokollet skall vara straffbara på försöksstadiet.

Artikel 3 behandlar spridning av rasistiskt och främlingsfientligt material med hjälp av datorsystem. Parterna skall straffbelägga gärningar som består i att till allmänheten sprida eller på annat sätt göra tillgängligt rasistiskt och främlingsfientligt material med hjälp av datorsystem. Med uttrycket ”göra tillgängligt” avses bl.a. att göra materialet tillgängligt on line för andra. Uttrycket täcker även förfarandet att skapa och kompilera hyperlänkar i syfte att underlätta andras tillgång till rasistiskt material (se den förklarande rapporten punkt 28).

En part får förbehålla sig rätten att inte införa straffansvar när materialet förespråkar, främjar eller uppmuntrar diskriminering utan samband med hat eller våld, under förutsättning att det finns andra effektiva motåtgärder. Vidare har en part möjlighet att förbehålla sig rätten att inte tillämpa artikeln i sådana fall av diskriminering där det, på grund av etablerade principer om yttrandefrihet i partens rättssystem, inte kan föreskrivas åtgärder.

I *artikel 4* behandlas hot som är rasistiskt och främlingsfientligt motiverade. Parterna skall straffbelägga gärningar som består i att med hjälp av ett datorsystem antingen hota personer av det skälet att de kännetecknas av en viss ras, hudfärg, härstamning eller nationellt eller etniskt ursprung eller trosbekännelse, eller att hota en grupp av personer som särskiljs på sätt som nyss har sagts, med att begå vad som enligt partens nationella lagstiftning är ett allvarligt brott. I motsats till vad som är fallet med artiklarna 3, 5 och 6, som tar sikte på förfaranden riktade till allmänheten, omfattar artikel 4 även hot som framförs vid privat kommunikation. Artikeln ger inte möjlighet till något undantag eller förbehåll.

Artikel 5 handlar om kränkningar som är rasistiskt eller främlingsfientligt motiverade. Kriminaliseringen skall omfatta gärningar som består i att offentligen med hjälp av ett datorsystem kränka antingen personer av det skälet att de tillhör en grupp som kännetecknas av viss ras, hudfärg, härstamning eller nationellt eller etniskt ursprung eller trosbekännelse, eller en grupp av personer som särskiljs genom något av dessa kännetecken. En part får antingen uppställa krav på att brottet resulterar i att personen eller gruppen av personer utsätts för hat, missaktning eller löje eller förbehålla sig rätten att helt eller delvis inte tillämpa artikeln.

I *artikel 6* behandlas spridning av visst material som rör folkmord eller brott mot mänskligheten. Varje part skall straffbelägga gärningar som består i att med hjälp av ett datorsystem till allmänheten sprida eller på annat sätt göra tillgängligt material som förnekar, grovt förringar, gillar eller rättfärdigar gärningar som utgör folkmord eller brott mot mänskligheten. Det skall vara fråga som folkmord eller brott mot mänskligheten så som dessa gärningar definieras i folkrätten och som har erkänts genom lagakraftvunna beslut i vissa internationella domstolar. Syftet med bestämmelsen är att slå fast att fakta beträffande vissa välbelagda historiska skeenden inte skall kunna förnekas, förringas, förhärligas eller rättfärdigas.

En part har möjlighet att antingen uppställa krav på att förnekande eller grovt förringande görs med uppsåt att uppmuntra till hat, diskriminering eller våld mot en enskild person eller en grupp av personer under åberopande av ras, hudfärg, härstamning eller nationellt eller etniskt ursprung eller trosbekännelse eller att förbehålla sig rätten att helt eller delvis inte tillämpa artikeln.

Medhjälp behandlas i *artikel 7*. Enligt denna artikel skall uppsåtlig medhjälp till brott som straffbeläggs i enlighet med protokollet kriminaliseras, om gärningsmannens syfte är att ett sådant brott skall begås.

5.2.4 Övriga bestämmelser

I *artikel 8*, som behandlar förhållandet mellan konventionen och tilläggsprotokollet, föreskrivs att följande artiklar i konventionen i tillämpliga delar skall gälla även för protokollet:
- artikel 1 som innehåller definitioner,
- artikel 12 om juridiska personers ansvar,
- artikel 13 om påföljder och åtgärder,
- artikel 22 om jurisdiktion,
- artikel 41 om federala stater,
- artikel 44 om ändringar,
- artikel 45 om tvistlösning samt
- artikel 46 om samråd mellan parterna.

Vidare skall parterna utvidga tillämpningsområdet för de processrättsliga bestämmelserna i artiklarna 14-21 i konventionen och bestämmelserna om internationellt samarbete i artiklarna 23-35 till att gälla även artiklarna 2-7 i protokollet.

Enligt *artikel 9* står det öppet för alla som har undertecknat konventionen att även underteckna tilläggsprotokollet. I artikeln anges hur detta skall ske. Det är således inte möjligt att tillträda enbart tilläggsprotokollet.

Artikel 10 behandlar ikraftträdande och *artikel 11* rör anslutning till protokollet efter att detta har trätt i kraft.

Enligt *artikel 12* gäller förbehåll och förklaringar som har avgetts rörande bestämmelser i konventionen också för tilläggsprotokollet, om inte parten förklarar något annat. Där anges vidare i vilken utsträckning parterna får förklara att de utnyttjar möjligheten att ställa upp särskilda rekvisit, nämligen i fråga om artiklarna 3, 5 och 6. Vidare har en part möjlighet att göra förbehåll enligt två artiklar i konventionen, nämligen artikel 22 punkt 2 och artikel 41 punkt 1, oavsett tidigare förbehåll. Några andra förbehåll är inte tillåtna.

I *artikel 13* regleras återtagande av förbehåll. Protokollets territoriella tillämpning behandlas i *artikel 14*. Möjligheten till uppsägning av protokollet regleras i *artikel 15*. I likhet med konventionen kan tilläggsprotokollet sägas upp så snart en part önskar det. Meddelanden angående protokollet behandlas i *artikel 16*.

6 Konventionens överensstämmelse med svensk rätt

6.1 Allmänna utgångspunkter

Sverige tillhör de länder som tidigt införde en reglering av IT-användning. Vi ligger långt framme när det gäller kriminalisering av data- och datorrelaterade brott. En anpassning till konventionen kräver därför ganska få åtgärder på det straffrättsliga området. Däremot har den straffrättsliga regleringen av traditionella brott som exempelvis förfalskningsbrott inte till fullo anpassats till den moderna tekniska miljön. En översyn av kapitel 14 och 15 i brottsbalken har emellertid aviserats.

På det processrättsliga området har frågan om anpassningar av reglerna om tvångsmedel till modern teknisk miljö utretts av bl.a. Datastraffrättsutredningen (Information och den nya InformationsTeknologin; SOU 1992:110), Telelagsutredningen (Telelag; SOU 1992:70) och Buggningsutredningen (Om buggning och andra hemliga tvångsmedel; SOU 1998:46). De processrättsliga reglerna är dock i allt väsentligt oförändrade, med undantag för regleringen av hemliga tvångsmedel. Det behövs därför mer ingripande ändringar av den processrättsliga lagstiftningen än av den straffrättsliga för att möta konventionens krav. Reglerna om hemlig teleavlyssning har dock successivt förändrats och anpassats till teknikutvecklingen, och hemlig teleövervakning har införts som nytt tvångsmedel i RB (prop. 1988/89:124, 1994/95:227 och 2002/03:74).

Det internationella samarbetet har utvecklats mycket snabbt under senare år, såväl i fråga om polissamarbete som internationell rättslig hjälp i brottmål. En helt ny lagstiftning om interna-

tionell rättslig hjälp trädde i kraft den 1 oktober 2000. Vid tillkomsten av denna lagstiftning lades stor möda ner på att göra den så vidsträckt som möjligt för att möta framtida krav på fördjupat internationellt samarbete. Reglerna om rättslig hjälp gjordes tillämpliga även på sådana tvångsmedel som Sverige vid tidpunkten för lagstiftningsarbetet inte hade några bindande internationella åtaganden att bistå med. Även när det gäller internationell rättslig hjälp är således den svenska lagstiftningen redan väl anpassad till de krav som konventionen ställer. Behovet av ändringar i lagstiftningen om internationell rättslig hjälp hänger därför främst samman med vilka ändringar som krävs inom processrätten.

Huvudparten av de gärningar som enligt konventionen skall kriminaliseras är redan straffbara enligt svensk rätt. Straffansvaret är emellertid fördelat på ett antal olika bestämmelser och följer en helt annan systematik än konventionen. I vissa hänseenden är den svenska regleringen mera långtgående än vad konventionen kräver. I detta kapitel görs en jämförelse mellan åtagandena i konventionen och den nuvarande svenska lagstiftningen.

Vissa av brotten har en gradindelad straffskala med olika straffsatser för ringa brott respektive brott av normalgraden eller grovt brott. Tankarna bakom konventionen är att brott av ringa karaktär inte alltid måste lagföras, även om detta inte kommit till direkt uttryck i texten (se den förklarande rapporten punkt 37). Ställningstagandet skall ses mot bakgrund av att flertalet europeiska länder tillämpar den s.k. opportunitetsprincipen (som innebär att de brottsbekämpande myndigheterna har vida ramar att avgöra vad som skall beivras), medan svensk rätt bygger på legalitetsprincipen (som innebär att brott alltid skall beivras om det inte finns någon uttrycklig regel som föreskriver annat). Det förhållandet att vissa ringa brott inte har en tillräcklig straffskala för att uppfylla konventionens alla krav torde därför sakna praktisk betydelse. Det kan nämligen förutsättas att rättslig hjälp inte begärs när brottet är obetydligt och att andra länder inte ställer

krav på att gärningar som anses för obetydliga för att beivras av dem skall lagföras här i landet.

6.2 Brott riktade mot datorsystem och datorbehandlad information (artiklarna 2-5)

6.2.1 Bestämmelser om dataintrång och olovlig avlyssning m.m.

Bedömning: Straffbestämmelsen om dataintrång täcker inte helt det område som enligt konventionen skall kriminaliseras när det gäller införing och undertryckande av uppgifter samt allvarligt hindrande av datorsystemens funktion. Det finns inte heller någon straffbestämmelse som avser olovlig avlyssning av elektromagnetiska emissioner. För att uppfylla kraven i artiklarna 3, 4 och 5 krävs det lagstiftningsåtgärder.

Nuvarande bestämmelser

Reglerna i 4 kap. brottsbalken (BrB) om brott mot frihet och frid har ett komplicerat inbördes förhållande. Det är därför nödvändigt att redogöra för skyddet mot intrång i sin helhet.

Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande, döms enligt 8 § för *brytande av post- eller telehemlighet* till böter eller fängelse i högst två år. Genom bestämmelsen skyddas såväl meddelanden i traditionell form som elektroniska meddelanden. Meddelanden som befordras via radio faller däremot utanför det straffbara området. Skyddet gäller oavsett om innehållet består av ljud, bild, text eller annat. Skyddet för meddelandet sträcker sig från den tidpunkt när meddelandet har avlämnats för befordran till dess att meddelandet har nått mottagaren.

Den moderna tekniken innebär bl.a. att telefoni inte längre alltid förutsätter medverkan av ett telebefordringsföretag. I den

mån telemeddelanden befordras på annat sätt, t.ex. via privata kommunikationsnät, skyddas de inte av straffbestämmelsen.

Straffansvaret för meddelanden under befordran är alltså inte heltäckande.

Försök till brytande av post- eller telehemlighet är inte straffbart. Däremot är förberedelse till brytande av telehemlighet straffbar genom en särskild bestämmelse i 9 b §. Om någon anbringar ett tekniskt hjälpmedel med uppsåt att bryta telehemlighet på sätt som sägs i 8 § skall han dömas för förberedelse till sådant brott, under förutsättning att han inte har gjort sig skyldig till fullbordat brott. Straffet är böter eller fängelse i högst två år. Straffbestämmelsen i 9 b § torde uppfylla kravet på kriminalisering i stadierna före fullbordat brott.

I 9 § straffbeläggs som *intrång i förvar* att någon olovligen bryter brev eller telegram eller annars bereder sig tillgång till något som förvaras förseglat eller under lås eller annars tillslutet. Bestämmelsen är subsidiär till bestämmelsen om brytande av post- eller telehemlighet. Straffskyddet omfattar även brev och andra meddelanden som ännu inte har lämnats till befordran eller som redan har kommit mottagaren till handa. Straffet är böter eller fängelse i högst två år. Försök och förberedelse är inte belagd med straff. Bestämmelsen har inte något direkt intresse för konventionsåtagandena.

Olovlig avlyssning regleras i 9 a §. Där straffbeläggs att någon olovligen genom tekniskt hjälpmedel för återgivning av ljud i hemlighet avlyssnar eller tar upp tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst till vilken allmänheten inte har tillträde och som han inte själv deltar i eller som han obehörigen har berett sig tillträde till. Regeln är subsidiär till straffbestämmelsen om brytande av post- eller telehemlighet. Straffet är böter eller fängelse i högst två år. Försök är inte belagt med straff, medan förberedelse faller in under den tidigare nämnda särskilda förberedelsebestämmelsen i 9 b §. Bestämmelsen om olovlig avlyssning skyddar således andra intressen än vad som avses i konventionens artikel 3.

Bestämmelsen om *dataintrång*, som ursprungligen fanns i datalagen, finns numera i brottsbalken. I 9 c § straffbeläggs som dataintrång att någon olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning. Straffansvaret omfattar såväl påverkan på informationen som på de program som styr databehandlingen. Bestämmelsen innehåller inte något effektrekvisit och kan därför tillämpas på alla fall där en gärning riktas mot datorer och data. Det finns inte heller något krav på att intrånget har inneburit ett kringgående av säkerhetsåtgärder. Det saknar vidare betydelse om upptagningen finns i en enskild dator eller i ett nät. Straffansvaret täcker således varje form av intrång som är olovligt.

Med upptagning för automatisk databehandling avses även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling. Detta innebär bl.a. att den information som är på väg att matas in skyddas.

Straffregeln om dataintrång är subsidiär till reglerna om brytande av post- eller telehemlighet och intrång i förvar. Straffet är böter eller fängelse i högst två år.

Försök och förberedelse till dataintrång, som om det fullbordats inte skulle ha varit ringa, är straffbart enligt 10 §.

Täcker de nuvarande reglerna konventionens krav?

Av det nyss sagda framgår att det redan finns straffbestämmelser som täcker kraven i artikel 2 på straffansvar för olovligt intrång. Även kravet på ansvar för försök till sådant brott är uppfyllt.

När det gäller avlyssning av datorbehandlingsbara uppgifter är läget ett annat.

En dator som används ger ofrivilligt ifrån sig signaler som kan tolkas med hjälp av teknisk utrustning. Detta är något som ibland betecknas som elektromagnetiska emissioner men som i Sverige ofta benämns röjande signaler (RÖS). Genom att av-

lyssna dessa signaler går det att få kunskap dels om vad som bearbetas i datorn, dels om åtkomstkoder.

Det finns för närvarande inte någon straffbestämmelse i svensk rätt som tar sikte på annan olovlig avlyssning än sådan som äger rum vid överföring av datorbehandlingsbara uppgifter. Sådan överföring kan vara straffbar antingen som brytande av telehemlighet, om det är fråga om överföring via ett allmänt kommunikationsnät, eller som dataintrång, om det är fråga om en överföring via ett elektroniskt hjälpmedel till en dator (t.ex. från ett tangentbordet till en hårddisk). I övrigt är olovlig avlyssning av datorbehandlingsbara uppgifter inte straffbar. För att uppfylla kraven i artikel 3 krävs det därför lagstiftningsåtgärder.

Straffansvaret för dataintrång och brytande av telehemlighet täcker också till största delen det område som kriminaliseringen skall omfatta enligt artiklarna 4 och 5. Som tidigare har nämnts är det straffbelagt att ändra eller utplåna uppgifter, vilket får anses motsvara kraven på kriminalisering av handlande som innebär att datorbehandlingsbara uppgifter skadas, raderas, försämras eller ändras. Straffansvaret för försök och förberedelse får i dessa delar anses uppfylla kraven i artikel 11 punkt 2. Det sagda gäller dock inte försök och förberedelse till dataintrång som om det hade fullbordats skulle har varit att anse som ringa. För att helt uppfylla kraven i konventionen måste Sverige antingen utvidga straffansvaret för försök till alla typer av dataintrång eller utnyttja möjligheten till förbehåll.

De nuvarande straffbestämmelserna motsvarar dock inte hela det område som enligt konventionens artiklar 4 och 5 skall vara kriminaliserat. Att tillfälligt hindra ett datasystem från att fungera normalt, t.ex. genom s.k. tillgänglighetsattacker (se närmare om detta i avsnitt 9), är inte straffbart som dataintrång.

Däremot kan, om gärningen vållar skada, den eventuellt leda till straffansvar för skadegörelse, under förutsättning att den vållar skada på ett fysiskt föremål och att skadan omfattas av gärningsmannens uppsåt (se nästa avsnitt). Om en sådan skadegörande handling riktar sig mot vitala samhällsintressen torde ansvar för sabotage kunna komma i fråga. Regleringen är dock inte

heltäckande, varför hindrandet som sådant kan falla utanför vad som för närvarande är straffbart enligt svensk rätt.

Det finns inte heller någon straffbestämmelse som tar sikte på att datorbehandlad information endast undertrycks eller på annat sätt görs oåtkomlig. Som framgår av det följande är regeln om undertryckande av urkund tillämplig endast i de fall där en ett elektroniskt dokument uppfyller kraven på att vara en urkund. Vissa andra straffbestämmelser torde under speciella omständigheter kunna aktualiseras (se nästa avsnitt). Den nuvarande lagstiftningen är emellertid inte tillräcklig för att i alla delar uppfylla kraven i konventionen.

Även i ett annat avseende är den nuvarande kriminaliseringen otillräcklig i förhållande till artikel 4, nämligen när gärningen består i att datasystemet olovligen tillförs information. För närvarande är ett sådant handlande straffbart endast om uppgifterna förs in i ett register.

Det krävs alltså viss komplettering av den nuvarande lagstiftningen för att Sverige helt skall uppfylla kraven i artiklarna 4 och 5.

Rambeslut om angrepp mot informationssystem

Inom Europeiska unionen har upprättats ett utkast till rambeslut om angrepp mot informationssystem (EGT C 203 E, 27.8.2002, s. 109). Rambeslutet skall ses mot bakgrund av behovet av att, i en alltmer IT-beroende värld, skapa gemensamma regler för att kunna bekämpa högteknologisk brottslighet. Europarådets konvention om IT-relaterad brottslighet har i vissa avseenden tjänat som förebild för rambeslutet.

Rambeslutet innehåller bestämmelser om vilka förfaranden som skall vara straffbelagda som angrepp mot informationssystem. I fråga om kriminaliseringens omfattning överensstämmer rambeslutet till stora delar med konventionen om IT-relaterad brottslighet. Rambeslutet innehåller emellertid även bestämmelser om vilka påföljder dessa brott skall kunna leda till. Dessutom

finns det bestämmelser om bl.a. ansvar och påföljder för juridiska personer, om jurisdiktion och om informationsutbyte.

Regeringen överlämnade den 27 maj 2004 en proposition till riksdagen med förslag om att riksdagen skulle godkänna utkastet till rambeslut. Propositionen innehöll inte några lagförslag. Dessa kommer att presenteras i senare sammanhang. Regeringen framhöll emellertid i propositionen att svensk rätt till övervägande del uppfyller rambeslutets krav på vilka handlingar som skall vara straffbelagda (prop. 2003/04:164 s. 23 ff).

Rambeslutet och de lagändringar som krävs för antagandet behandlas i promemorian Angrepp mot informationssystem (Ds 2005:5. Förslagen presenteras närmare i kapitel 10.

6.2.2 Skadegörelse och vissa andra brott som rör påverkan på datorsystem och information i dessa

Bedömning: Förutom reglerna i 4 kap. finns det bestämmelser i andra kapitel i brottsbalken som, beroende på omständigheterna, ibland kan tillämpas på några av de förfaranden som regleras i artiklarna 4 och 5. Dessa straffbestämmelser är dock av underordnad betydelse i sammanhanget och någon ändring av dem är inte påkallad.

Nuvarande bestämmelser om skadegörelse

Vissa av de beteenden som anges i artiklarna 4 och 5 faller, som nyss nämnts, formellt in under straffbestämmelserna om skadegörelsebrott. I 12 kap. 1 § BrB straffbeläggs som *skadegörelse* att någon skadar fast eller lös egendom till men för annans rätt. Straffskalan är, från den 1 januari 2004, böter eller fängelse i högst ett år (prop. 2002/03:138, bet. 2003/04:JuU3).

Om brottet är grovt döms för *grov skadegörelse* till fängelse i högst fyra år (12 kap. 3 § BrB). Vid bedömningen av om brottet är grovt skall särskilt beaktas bl.a. om skadan drabbat sak av stor

kulturell eller ekonomisk betydelse eller om skadan annars är särskilt kännbar.

Är brottet med hänsyn till värdet och övriga omständigheter ringa döms enligt 12 kap. 2 § BrB för *åverkan* till böter.

Försök och förberedelse till grov skadegörelse och försök till skadegörelse samt underlåtenhet att avslöja grov skadegörelse är straffbara (12 kap. 5 § BrB). Däremot är förberedelse till brott av normalgraden och försök och förberedelse till åverkan inte straffbelagd.

Det som kan bli föremål för skadegörelse är egendom som har fysisk substans. Tillämpningsområdet omfattar således inte immateriell egendom. Datorbehandlingsbara uppgifter räknas till den senare kategorin,[29] medan dataanläggningar och fysiska databärare hör till den förra.

Täcker reglerna om skadegörelse konventionens krav?

Skadegörande angrepp som riktar sig mot de fysiska delarna av en datoranläggning eller medium för lagring av datainformation kan bestraffas som skadegörelse i likhet med angrepp på vilket slags lös egendom som helst. Hur långt straffansvaret för skadegörelse sträcker sig när det gäller information är däremot oklart. Diskussionen om skadegörande angrepp har främst tagit sikte på sådan information som finns på en fysisk bärare.

När Förmögenhetsbrottsutredningen behandlade frågan om straffansvar för angrepp mot datorer utgick den från att skadegörande angrepp på mjukvara uppfyllde rekvisiten för skadegörelse om databäraren förstördes (SOU 1983:50 s. 182 f).[30] Utredningen ansåg även att angrepp som bara innebär att informationen förstörs kan bedömas som skadegörelse. Varje utplånande av lagrade data kunde dock enligt utredningen inte innefatta skadegörelse. För ansvar för skadegörelse borde krävas att utplånade data utgjorde en väsentlig del av den på databäraren lagrade in-

[29] Datastraffrättsutredningen betecknade information av det slaget som ”kvasimateriell”. Det innebär dock inte någon skillnad i detta fall.
[30] Resonemanget byggde på dåtidens teknik med lagring på magnetband.

formationen, medan ansvar för dataintrång kunde aktualiseras i andra fall.[31] Departementschefen ställde sig bakom utredningens uttalanden (prop. 1985/86:65 s. 12 f).

Datastraffrättsutredningen framhöll att skadegörelse inte bara kan drabba datorer och databärare utan även olika slag av kommunikationsutrustning (SOU 1992:110 s. 207). Vidare påpekade utredningen att föreställningen att det krävs omfattande ändringar eller raderingar för att gärningen skall vara straffbar som skadegörelse leder till icke godtagbara resultat eftersom även enstaka ändringar kan leda till exempelvis att ett helt program blir oanvändbart. Utredningen pekade också på att en diskett har ett obetydligt ekonomiskt värde medan den information som den innehåller kan representera ett mycket högt värde. Datastraffrättsutredningen föreslog att det skulle införas en särskild bestämmelse om dataskadegörelse, bestående i att någon olovligen utplånar, ändrar eller undertrycker data för automatisk databehandling. Förslaget har inte lett till någon lagstiftning.

Utgångspunkten för reglerna om skadegörelse är att det krävs en fysisk handling som leder fram till skadan (Lena Holmqvist m.fl. Brottsbalken. En kommentar s. 12:3). Vid fysiska angrepp på hård- eller mjukvara är det kravet uppfyllt. Det kan däremot diskuteras om en sådan åtgärd som att skriva in ett kommando på ett tangentbord och med hjälp av detta sända en instruktion till en annan dator uppfyller kravet på fysisk handling. Det finns inte någon rättspraxis som belyser denna frågeställning. De ursprungliga förarbetena ger av naturliga skäl inte heller någon ledning, eftersom angrepp mot datorer inte existerade när regeln kom till.

En straffregel har emellertid inte ett statiskt innehåll. Reglerna är skrivna för att kunna tillämpas även om tekniken och andra förutsättningar ändras. Ett exempel på detta är att åtskilliga av de befintliga straffbestämmelserna avseende förmögenhetsbrott kan tillämpas oberoende av datoriseringen.

[31] Vid den tidpunkten var bestämmelsen om dataintrång subsidiär till brottsbalkens regler.

Det kan konstateras att det grundläggande krav som Förmögenhetsbrottsutredningen ställde upp för att en gärning riktad mot information skall betraktas som skadegörelse ter sig helt otidsenligt, så som tekniken har utvecklats. Det är uppenbart att även en mycket liten ändring eller utplånande av enstaka uppgifter kan leda till betydande skada om den nämligen avser någon vital uppgift eller drabbar ett program. De motivuttalanden som gjordes med utgångspunkt i en numera föråldrad teknik kan därför inte tillmätas någon avgörande betydelse när det gäller att bedöma straffansvarets räckvidd.

Det torde också väl kunna hävdas att de relativt begränsade åtgärder som krävs för att med hjälp av en dator åstadkomma skada i ett datorsystem kan jämföras med ett fysiskt handlande. Å andra sidan är behovet av att kunna som skadegörelse bestraffa förfaranden som innebär att information skadas eller förstörs mycket begränsat. Eftersom bestämmelsen om dataintrång täcker den situationen att någon ändrar eller utplånar data blir utrymmet för att bedöma angrepp mot information i datorer och datasystem som skadegörelse mycket litet. Reglerna om skadegörelse är därför tämligen ointressanta när det är fråga om skadegörande påverkan på informationen.

Ett annat skäl till att frågan om ansvar för skadegörelse sällan aktualiseras kan vara straffskalornas utformning. Eftersom skadegörelse som är ringa eller av normalgraden även efter lagändringen den 1 januari 2004 har en straffskala som är lägre än den för dataintrång och övriga bestämmelser i 4 kap. BrB som kan aktualiseras vid intrång i datorsystem eller påverkan på information konsumeras skadegörelsen normalt av det grövre brottet. Om det primära syftet med handlandet är att åstadkomma skada torde dock ansvar för skadegörelse kunna utkrävas. Om gärningen orsakar allvarlig skada kan, beroende på omständigheterna, ansvar för grov skadegörelse aktualiseras vid sidan av ansvar för intrånget. Något behov av ändring i bestämmelserna om skadegörelse finns således inte.

Andra bestämmelser som kan vara tillämpliga

Bestämmelsen om *sabotage* (13 kap. 4 § BrB), som bl.a. straffbelägger att någon genom skadegörelse eller annan åtgärd allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon eller dylikt allmänt hjälpmedel torde också kunna tillämpas. Under straffansvaret för sabotage hänförs bl.a. gärningar som innebär att någon förstör eller skadar egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning. Ett dataintrång som syftar till att förstöra eller allvarligt hindra funktionen i datorsystem av vital betydelse för landet kan således falla under straffansvaret för sabotage. Straffet för sabotage är fängelse i högst fyra år. Är brottet grovt döms för grovt sabotage till fängelse lägst två och högst tio år eller på livstid (13 kap. 5 § BrB). Försök och förberedelse till sabotage och grovt sabotage är straffbart (13 kap. 12 § BrB).

Det kan vidare diskuteras om straffbestämmelser i 8 och 10 kap. BrB kan vara tillämpliga. För *egenmäktigt förfarande* (8 kap. 8 § BrB) döms bl.a. den som utan tillgrepp, genom att bryta eller anbringa lås eller på annat sätt olovligen rubbar annans besittning. Straffet för egenmäktigt förfarande är böter eller fängelse i högst sex månader. Om brottet är grovt är straffet fängelse i högst två år. Beroende på hur gärningen har utförts kan ansvar för egenmäktigt förfarande eventuellt aktualiseras vid åtgärder som innebär att viss information görs oåtkomlig eller mycket svårtillgänglig. Detta förutsätter dock att gärningen har riktats mot en fysisk databärare eftersom brott enligt 8 kap. BrB endast kan avse något som har fysisk substans. Utrymmet för att tillämpa regeln om egenmäktigt förfarande är därför mycket litet. Med tanke på den låga straffskalan för brott av normalgraden och att försök och förberedelse till egenmäktigt förfarande inte är straffbelagt är dessutom den bestämmelsen inte tillräcklig för att uppfylla konventionens krav.

Om någon, som har tillgång till ett datorsystem, olovligen brukar detta och därigenom vållar skada eller olägenhet kan han enligt 10 kap. 7 § BrB dömas för *olovligt brukande* till böter eller

fängelse i högst ett år. Är brottet grovt är straffet fängelse lägst sex månader och högst fyra år. Försök och förberedelse är inte straffbelagt.

Man kan tänka sig fall där någon gör sig skyldig till olovligt brukande, t.ex. använder arbetsgivarens system för elektronisk post för privat bruk, i så stor omfattning att det påverkar kapaciteten i datorsystemet eller hindrar inkommande meddelanden. Den information som finns i systemet kan då bli oåtkomlig eller svårtillgänglig för andra användare.

De nu redovisade straffbestämmelserna torde således under speciella omständigheter kunna tillämpas på förfaranden som regleras i artiklarna 4 och 5. I allt väsentligt är det dock reglerna i 4 kap. BrB som står för skyddet mot gärningar riktade mot datorsystem och information i dessa. Några ändringar i de regler som nu har redovisats torde därför inte vara påkallade.

6.3 Förfalskningsbrott (artikel 7)

Bedömning: Det krävs lagstiftningsåtgärder för att uppfylla kraven i artikel 7 på kriminalisering av dataförfalskning.

6.3.1 Nuvarande bestämmelser

Den som, genom att skriva annan, verklig eller diktad, persons namn eller genom att falskeligen skaffa sig annans underskrift eller på annat sätt framställer falsk urkund eller falskeligen ändrar eller fyller ut en äkta urkund, döms för *urkundsförfalskning* (14 kap. 1 § BrB). Ett grundläggande krav för att gärningen skall vara straffbar är att åtgärden har inneburit fara i bevishänseende. Straffet för urkundsförfalskning är fängelse i högst två år.

För *grov urkundsförfalskning* döms till fängelse, lägst sex månader och högst sex år (14 kap. 3 § BrB). Vid bedömningen av om brottet är grovt skall särskilt beaktas om förfalskningen har avsett myndighets arkivhandling av vikt eller urkund som är särskilt betydelsefull i den allmänna omsättningen. Som exempel på

det senare nämns obligation, aktiebrev och inteckningshandling. Ett annat skäl att bedöma gärningen som grov kan vara att gärningen annars varit av särskilt farlig art.

Om urkundsförfalskning är att anse som ringa döms för *förvanskning av urkund* till böter eller fängelse i högst sex månader (14 kap. 2 § BrB). Vid bedömningen av om gärningen är ringa skall särskilt beaktas om urkunden är av mindre vikt. Som exempel på detta nämns kassakvitto, kontramärke eller dylikt mottagningsbevis. Ett annat skäl att bedöma gärningen som ringa kan vara att gärningen skett för att hjälpa någon till hans rätt.

Försök och förberedelse till urkundsförfalskning och grov urkundsförfalskning är straffbar(14 kap. 12 § BrB). Detta gäller dock inte om brottet, om det hade fullbordats, skulle ha varit att anse som ringa. Försök och förberedelse till förvanskning av urkund är inte heller straffbelagt.

Den som förstör, gör obrukbar eller undanskaffar urkund, över vilken han vid tillfället inte har rätt att förfoga så, döms, om åtgärden innebär fara i bevishänseende, för *undertryckande av urkund* (14 kap. 4 § BrB). Straffet är fängelse i högst två år. Om gärningen är ringa är straffet böter eller fängelse i högst sex månader. Om brottet är grovt bestraffas det med fängelse i lägst sex månader och högst fyra år.

Försök och förberedelse till undertryckande av urkund är straffbar (14 kap. 12 § BrB). Detta gäller dock inte om brottet, om det hade fullbordats, skulle ha varit att anse som ringa.

6.3.2 Uppfyller elektroniska dokument kraven på att vara förfalskningsobjekt?

Straffbestämmelserna i 14 kap. BrB skyddar, som framgått av det sagda, urkunder. För att en handling skall betraktas som en urkund måste den uppfylla vissa grundläggande krav.

Den skall för det första ha ett föreställningsinnehåll, dvs. förmedla tankar, fakta eller annat. Vidare skall den ha upprättats till bevis eller annars kunna ha betydelse som bevis. Till urkunder räknas bl.a. protokoll, kontrakt, skuldebrev, intyg och andra

handlingar, som har upprättats till bevis eller som annars är av betydelse som bevis. Hit hör också legitimationskort samt biljetter och liknande bevismärken. Det krävs också att handlingen skall ha en viss varaktighet samt att det skall vara möjligt att ta del av innehållet i den, normalt genom att läsa detta.

Handlingen skall vidare ha en utställare som direkt eller indirekt kan utläsas av handlingen. Det skall således vara möjligt att identifiera den som står bakom innehållet i handlingen. Vissa handlingar som helt saknar utställarangivelse, t.ex. obestyrkta avskrifter, fotokopior och liknande anses inte vara urkunder.

En handling i elektronisk form saknar i de flesta fall en utställare av det slag som krävs för ansvar enligt 14 kap. BrB. Förfalskning av elektroniska dokument som inte har förts över till pappersform och då fått urkundsstatus, t.ex. genom att utställaren har undertecknat detta, faller därför normalt utanför straffansvaret för urkundsförfalskning. Elektroniska dokument kan emellertid numera förses med s.k. elektronisk signatur, som är avsedd att motsvara en namnteckning. Om ett elektroniskt dokument, som på det sättet har en tydlig utställare, förfalskas torde straffansvar för urkundsförfalskning kunna utkrävas. De allra flesta elektroniska dokument har dock, i likhet med exempelvis en obestyrkt fotokopia, inte en tillräckligt tydlig utställare för att uppfylla det grundläggande kravet på en urkund. Därmed skyddas de inte heller av straffbestämmelserna om förfalskning.

Det kan emellertid vara brister i andra grundläggande kriterier som gör att en handling i elektronisk form inte uppfyller kraven på en urkund och därmed inte heller kan vara ett förfalskningsobjekt. Något som ofta framhålls i detta sammanhang är kravet på varaktighet. Ett elektroniskt dokument som inte har fixerats på ett medium som omöjliggör ändringar anses inte uppfylla detta krav.

Information i elektronisk form har dessutom ofta inte ens formen av en handling. Den utgörs av lagrade data som vid behov kan sammanställas till en eller flera handlingar. Man talar därför om att lagrad datorbehandlad information utgör potentiella handlingar (se SOU 1992:110 s. 108 och 1997:39 s. 484). In-

nan innehållet har sammanställts och materialiserats kan manipulationer med informationen uppfylla kraven för straffansvar för dataintrång men däremot inte utgöra förfalskningsåtgärder eftersom informationen inte utgör ett förfalskningsobjekt.

Av samma skäl som reglerna om förfalskning av urkunder sällan kan tillämpas på information i elektronisk form kan ansvar för undertryckande av urkund sällan komma i fråga.

För att uppfylla kraven i artikel 7 krävs det alltså lagstiftningsåtgärder.

6.4 Bedrägeribrott (artikel 8)

Bedömning: De nuvarande reglerna uppfyller kraven på kriminalisering av databedrägeri, utom bestämmelsen om försök till ringa brott.

För *bedrägeri* döms enligt 9 kap. 1 § BrB den som genom vilseledande förmår någon till handling eller underlåtenhet som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställe denne är. Straffet är fängelse i högst två år.

För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift eller ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatiserad informationsbehandling eller någon annan liknande automatiserad process, så att det innebär vinning för gärningsmannen och skada för någon annan.

Är brottet grovt döms för *grovt bedrägeri* till fängelse lägst sex månader och högst sex år (9 kap. 3 § BrB). Vid bedömningen av om brottet är grovt skall bl.a. beaktas om gärningen varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada eller om gärningsmannen har begagnat falsk handling.

Är brottet med hänsyn till skadans omfattning och övriga omständigheter vid brottet att anse som ringa döms för *bedrägligt beteende* till böter eller fängelse i högst sex månader (9 kap. 2 § BrB).

Försök och förberedelse till bedrägeri och grovt bedrägeri är straffbart (9 kap. 11 § BrB), medan ringa brott inte är straffbelagda på dessa stadier.

Den befintliga lagstiftningen täcker kraven i artikel 8. Vidare täcks kravet på ansvar för försök i artikel 11 punkt 2, utom i fråga om ringa brott. För att uppfylla kraven i konventionen måste Sverige därför antingen utvidga straffansvaret för försök till ringa brott eller utnyttja möjligheten till förbehåll.

6.5 Barnpornografibrott (artikel 9)

Bedömning: De nuvarande reglerna om barnpornografibrott uppfyller kraven i konventionen, utom i fråga om försök till ringa brott.

6.5.1 Nuvarande bestämmelser

Bestämmelserna om straffansvar för barnpornografibrott finns i 16 kap. 10 a § BrB. Straffansvaret träffar den som

- skildrar barn i pornografisk bild,
- sprider, överlåter, upplåter, förevisar eller på annat sätt gör en sådan bild av barn tillgänglig för annan,
- förvärvar eller bjuder ut en sådan bild av barn,
- förmedlar kontakter mellan köpare och säljare av sådana bilder av barn eller vidtar någon annan liknande åtgärd som syftar till att främja handel med sådana bilder, eller
- innehar en sådan bild av barn.

Straffansvaret omfattar bilder av alla slag, bl.a. bilder i tryckta skrifter, fotografier och tecknade bilder men även bilder i videogram och bilder som förmedlats med TV-teknik. Bilder i elektronisk form omfattas således redan av straffbestämmelsen.

Ansvaret är inte begränsat till bilder där barn är inbegripna i handlingar som uppenbart har en sexuell innebörd. Pornografiska bilder där barn förekommer tillsammans med en eller flera

vuxna som utför sexuella handlingar omfattas också av kriminaliseringen. Även en bild där ett barn framställs på ett sätt som är ägnat att vädja till sexualdriften kan i vissa fall träffas av straffansvar. För att en bild av ett barn skall vara straffbar krävs att den enligt vanligt språkbruk och allmänna värderingar är pornografisk.

Med barn avses i straffbestämmelsen en person vars pubertetsutveckling inte är fullbordad eller som, när det framgår av bilden och omständigheterna kring den, är under 18 år.

Från det straffbara området för skildring och innehav har undantagits den som tecknar, målar eller på något annat liknande hantverksmässigt sätt framställer en bild som i sig uppfyller de objektiva rekvisiten för barnpornografi, om bilden inte är avsedd att spridas, överlåtas, upplåtas, förevisas eller på annat sätt göras tillgänglig för andra. Undantaget har tillkommit för att inte hindra framställningen av konstnärliga alster. Undantaget för hantverksmässigt framställda bilder torde sakna intresse i detta sammanhang eftersom konventionen endast behandlar brott som begås med hjälp av datorsystem. När undantaget tillkom framhölls att detta inte gäller för bilder som ritats eller på annat sätt framställts med hjälp av en datorteknik (prop. 1997/98:43 s. 81). Ett skäl till detta var att bilder i elektronisk form kan lagras, bearbetas och distribueras i det närmaste obegränsat. Ett annat var svårigheten att skilja mellan ett verkligt fotografi som överförts till elektronisk form, en bild som framställts i elektronisk form genom manipulation av ett sedvanligt fotografi och ett ”pseudofotografi” som framställts enbart genom dataanimation.

Även i andra fall skall en gärning inte utgöra brott, om gärningen med hänsyn till omständigheterna var försvarlig. Eftersom konventionen utgår från att endast gärningar som begås orättmätigt skall kriminaliseras torde detta begränsade undantag inte skapa något problem.

Den som i yrkesmässig verksamhet eller annars i förvärvssyfte av oaktsamhet sprider en barnpornografisk bild döms också för barnpornografibrott.

Straffet för barnpornografibrott är fängelse i högst två år eller, om brottet är ringa, böter eller fängelse i högst sex månader. Straffansvaret omfattar försök till brott under förutsättning att gärningen, om den hade fullbordats, inte skulle ha varit att bedöma som ringa (16 kap. 17 § BrB).

Straffet för grovt barnpornografibrott är fängelse i lägst sex månader och högst fyra år. Vid bedömningen av om brottet är grovt skall särskilt beaktas om det har begåtts yrkesmässigt eller i vinstsyfte, utgjort ett led i brottslig verksamhet som utövats systematiskt eller i större omfattning, avsett en särskilt stor mängd bilder eller avsett bilder där barn utsätts för särskilt hänsynslös behandling. Straffansvaret omfattar även försök och förberedelse.

Förberedelse till barnpornografibrott av normalgraden är inte straffbelagd och inte heller försök och förberedelse till ringa brott.

Barnpornografibrott omfattades tidigare av tryckfrihetsförordningens (TF) och yttrandefrihetsgrundlagens (YGL) tillämpningsområden. Alla bestämmelser om barnpornografibrott i dessa lagar har emellertid upphävts och det anges uttryckligen att grundlagarna inte skall tillämpas på pornografiska bilder (se 1 kap. 10 § TF och 1 kap. 13 § YGL). Däremot kan grundlagarna fortfarande tillämpas på pornografisk text utan samband med bilder.

In- och utförsel av barnpornografi är straffbar enligt lagen (1998:1443) om införsel och utförsel av barnpornografi. Ansvarsbestämmelserna finns i lagen (2000:1225) om straff för smuggling.

I lagen (1998:112) om ansvar för elektroniska anslagstavlor finns det också regler som syftar till att förhindra spridning av barnpornografi. Med elektronisk anslagstavla avses en tjänst för elektronisk förmedling av meddelanden i form av text, bild, ljud eller annan information. Den som tillhandahåller en elektronisk anslagstavla är skyldig att hålla uppsikt över innehållet på denna (4 §). I uppgiften ingår också att ta bort eller på annat sätt förhindra spridning av vissa meddelanden med brottsligt innehåll,

bl.a. barnpornografi (5 § första stycket 1). Den som uppsåtligen eller av grov oaktsamhet bryter mot denna skyldighet döms till böter eller fängelse i högst sex månader (7 §). Om brottet är grovt är straffet fängelse i högst två år. I ringa fall skall inte dömas till ansvar. Straffbestämmelsen är subsidiär till reglerna i brottsbalken (7 § andra stycket).

6.5.2 Täcker de nuvarande reglerna konventionens krav?

Svensk rätt uppfyller kraven på kriminalisering i artikel 9. Det nuvarande straffansvaret för barnpornografi är i själva verket i flera hänseenden mera långtgående än vad som krävs i konventionen. I princip är all hantering av barnpornografiska alster förbjuden. Vidare omfattar straffansvaret inte bara bilder som skildrar hur barnet deltar i ett uttalat sexuellt beteende utan även bilder där barnet har en passiv roll men förekommer i ett sexuellt färgat sammanhang. Ansvaret omfattar dessutom bilder av alla slag på alla typer av medier, medan konventionen enbart behandlar barnpornografi på datamedium. Även in- och utförsel är kriminaliserad. Som tidigare har nämnts hindrar konventionen inte en mera långtgående kriminalisering.

Enligt konventionens artikel 9 punkt 2 b skall straffansvaret även omfatta pornografiska alster som föreställer någon ”appearing to be minor”. Den nuvarande straffbestämmelsens utformning, som inte bygger på en absolut åldersgräns, torde uppfylla konventionens krav. Frågan om straffansvar för vad som brukar kallas anspelningspornografi (dvs. när vuxna personer framställs som barn eller förses med olika attribut för att påminna om barn) har för övrigt nyligen diskuterats i prop. 2003/04:12, med anledning av en liknande formulering i rambeslutet om åtgärder för att bekämpa sexuellt utnyttjande av barn och barnpornografi (a. prop. s. 32 f). Regeringen konstaterade där att det inte finns någon anledning att ändra på det tidigare synsättet att man inte generellt bör straffbelägga anspelningspornografi.

Den nuvarande lagstiftningen täcker också kraven i artikel 11 punkt 2 på ansvar för försök, utom i fråga om ringa brott. För

att uppfylla kraven i konventionen måste Sverige därför antingen utvidga straffansvaret till försök till ringa brott eller utnyttja möjligheten till förbehåll.

6.5.3 Rambeslut om åtgärder för att bekämpa sexuellt utnyttjande av barn och barnpornografi

I prop. 2003/04:12 har regeringen föreslagit riksdagen att anta ett inom Europeiska unionen upprättat utkast till rambeslut om åtgärder för att bekämpa sexuellt utnyttjande av barn och barnpornografi. Rambeslutet innehåller bl.a. en artikel om barnpornografi.

Några förslag till ändrad lagstiftning lades inte fram i propositionen. Regeringen gjorde dock den bedömningen att det materiella innehållet i straffbestämmelsen om barnpornografi i allt väsentligt täcker kraven i rambeslutet. Däremot ansågs det krävas justering av straffskalorna för vissa brott, bl.a. grovt barnpornografibrott. Behovet av lagändringar skulle övervägas i samband med beredningen av Sexualbrottskommitténs betänkande. Riksdagen har antagit propositionen (bet. 2003/04:JuU9).

I prop. 2004/05:45 presenterar regeringen förslag till en reformerad lagstiftning om sexualbrott som bl.a. innebär att 6 kap. BrB omarbetas helt, att det straffbara området för vissa brott utvidgas samt att straffskalorna för flera brott skärps. I fråga om grovt barnpornografibrott förslås att straffmaximum höjs från fängelse fyra år till fängelse sex år. Skälet till höjningen är framför allt att rambeslutet förutsätter att maximistraffet skall vara åtminstone fängelse fem år. Regeringens förslag om sex års straffmaximum stämmer enligt propositionen bättre överens med systematiken i brottsbalken och motiveras dessutom av det allmänna behovet av straffskärpning för sådana brott. Det är emellertid inte avsikten att ändringen av straffskalan skall leda till någon generell höjning av straffen för barnpornografibrott (a. prop s. 118 f). Ändringarna skall enligt förslaget träda i kraft den 1 april 2005.

6.5.4 Översyn av lagstiftningen om barnpornografibrott

Utredningen om kunskap om sexuellt exploaterade barn i Sverige har nyligen lagt fram sitt betänkande Sexuell exploatering av barn i Sverige (SOU 2004:71). Utredningen har föreslagit en översyn av lagstiftningen om barnpornografibrott i vissa avseenden. Som skäl för en översyn pekar utredningen bl.a. på det förhållandet att tillfällig nedladdning av barnpornografi på en dators temporära internetfil inte betraktas som innehav av barnpornografi och därmed faller utanför det straffbara området, vilket utredningen anser vara en brist.

Utredningens förslag bereds för närvarande i regeringskansliet. Inom ramen för detta övervägs hur lagstiftningen om barnpornografibrott kan förstärkas. Skärpningar i lagstiftningen om barnpornografibrott på det nu föreslagna sättet kommer självfallet att ytterligare förbättra möjligheterna att bekämpa sådan brottslighet som begås med hjälp av datorsystem.

6.6 Brott mot upphovsrätt m.m. (artikel 10)

Bedömning: Det krävs i detta sammanhang inte några ändringar i reglerna om upphovsrätt för att uppfylla åtagandena i konventionen.

6.6.1 Straffrättsliga regler

Reglerna om upphovsrätt innehåller såväl straffbestämmelser som andra sanktionsregler. Enligt 53 § lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (upphovsrättslagen) döms den som beträffande ett litterärt eller konstnärligt verk uppsåtligen eller av grov oaktsamhet vidtar åtgärder som innebär intrång i den till verket knutna upphovsrätten.

I 26 g och h §§ upphovsrättslagen finns det särskilda bestämmelser om hur datorprogram får användas utan att det kränker upphovsrätten. Där regleras t.ex. rätten att göra nödvändiga änd-

ringar i program, rätten till säkerhetskopiering m.m. Otillåtna åtgärder med datorprogram och vissa digitala sammanställningar regleras i 53 § andra stycket. Den som för eget bruk kopierar ett utgivet datorprogram eller ett program som har överlåtits med upphovsmannens samtycke skall inte dömas till ansvar, om förlagan för kopieringen inte används i näringsverksamhet eller offentlig verksamhet och han inte utnyttjar framställda exemplar av datorprogrammet för annat än enskilt bruk. Den som för enskilt bruk framställer exemplar i digital form av en offentliggjord sammanställning i sådan form skall inte heller dömas till ansvar under de förutsättningar som nyss har angetts.

Straffansvaret omfattar även den som till Sverige, för spridning till allmänheten, för in exemplar av verk, där exemplaret framställts utomlands under sådana omständigheter att en motsvarande framställning skulle ha varit straffbar här.

Straffet för upphovsrättsintrång är böter eller fängelse i högst två år. Försök och förberedelse till intrång i upphovsrätt är straffsanktionerade.

Brott mot upphovsrätt får åtalas av åklagare endast om målsäganden anger brottet till åtal eller om åtal är påkallat ur allmän synpunkt (59 § upphovsrättslagen).

Enligt 5 § första stycket 2 lagen om ansvar för elektroniska anslagstavlor (se avsnitt 6.5.1) omfattar skyldigheten att rensa bort eller att på annat sätt förhindra spridning av vissa meddelanden även meddelanden där det är uppenbart att användaren av anslagstavlan har gjort intrång i upphovsrätt genom att sända in meddelandet. Straffbestämmelsen i lagen om ansvar för elektroniska anslagstavlor är subsidiär till reglerna i upphovsrättslagen (7 § andra stycket).

6.6.2 Civilrättsliga åtgärder och sanktioner

Utöver straffbestämmelser innehåller upphovsrättslagen bl.a. regler om intrångsundersökning, vitesförbud, åtgärder med olovligt framställda varor m.m. och om skadestånd.

Det finns en särskild typ av tvångsåtgärd för att säkerställa bevisning om intrång i upphovsrätt, s.k. intrångsundersökning (56 a – g §§ upphovsrättslagen). Ett beslut om intrångsundersökning har stora likheter med ett domstolsbeslut om husrannsakan. Ett huvudskäl till att reglerna om intrångsundersökning infördes var att förbättra möjligheterna att säkra bevisning om upphovsrättsintrång i de fall där frågan inte blir föremål för brottsutredning. Åtgärden kan även tillämpas i fråga om försök och förberedelse. Beslut om intrångsundersökning meddelas av domstol på ansökan av upphovsmannen eller dennes rättsinnehavare (56 b §). Kronofogdemyndigheten ansvarar för verkställighet av sådana beslut (56 f §).

En domstol kan också, på yrkande av upphovsmannen eller hans rättsinnehavare eller annan som på grund av upplåtelse har rätt att utnyttja verket, vid vite förbjuda den som vidtar en åtgärd, som innebär intrång eller överträdelse, att fortsätta med åtgärden (53 a § upphovsrättslagen).

Den som begår upphovsrättsintrång kan även åläggas att mot lösen avstå intrångsföremålen och vissa hjälpmedel till upphovsmannen eller dennes rättsinnehavare. Alternativt kan domstolen, på yrkande av upphovsmannen eller dennes rättsinnehavare, förordna om att föremålen exempelvis skall ändras eller förstöras (55 § upphovsrättslagen).

Den som gör sig skyldig till intrång kan vidare åläggas att betala ersättning för utnyttjandet och att betala skadestånd (54 § upphovsrättslagen).

6.6.3 Aktuella förslag till ändringar

I en promemoria med förslag till omfattande ändringar i upphovsrätten (Ds 2003:35; Upphovsrätten i informationssamhället) behandlas åtskilliga frågor med anknytning till de frågor som tas upp i konventionens artikel 10. Förslagen i promemorian syftar till att stärka upphovsrätten samtidigt som de tillgodoser balansen mot viktiga allmänna intressen. Bakgrunden är att den digitala utvecklingen har lett till att upphovsrättsligt skyddade

verk enkelt och snabbt kan kopieras och överföras mellan olika länder, bl.a. via Internet. Förslagen bygger på två internationella fördrag, som har antagits av FN:s organ för immaterialrätt World Intellectual Property Organisation (WIPO), och på Europaparlamentets och rådets direktiv 2001/29/EG.

Förslagen innebär bl.a. att sådana förfaranden som syftar till att kringgå tekniska spärrar och andra tekniska åtgärder, vilkas ändamål är att förhindra intrång i upphovsrätt, förbjuds. En straffsanktion införs för sådana åtgärder som inte redan nu faller under straffansvaret för intrång i upphovsrätten.

I promemorian behandlas även frågan om svenskt tillträde till WIPO-fördragen. Den bedömning som görs är att det, utöver de lagstiftningsåtgärder som fordras för att genomföra direktivet, endast krävs marginella lagstiftningsåtgärder för en svensk ratificering av WIPO-fördragen (Ds 2003:35 s. 391 ff).

Regeringen har nyligen beslutat en lagrådsremiss baserad på promemorians förslag.

Vidare bör nämnas att det inom Justitiedepartementet har utarbetats en promemoria rörande utökade möjligheter att förverka utbyte och hjälpmedel vid brott (Ju2000/330/L5). Bakgrunden till förslagen är att Sverige har åtagit sig att begränsa sin tidigare avgivna förklaring till Europarådets konvention om penningtvätt, efterforskning, beslag och förverkande av vinning av brott (förverkandekonventionen) om att förverkande av vinning av brott samt hjälpmedel vid brott bara skall gälla vissa brott eller brottskategorier. I promemorian föreslås att det införs särskilda förverkandebestämmelser i de immaterialrättsliga författningarna. Förslaget innebär att det skapas möjlighet att förverka bl.a. egendom som har framställts genom intrång i immaterialrätt (eller värdet av sådan egendom). Även utbyte av brott skall kunna förverkas. Promemorian har remissbehandlats och övervägs nu inom regeringskansliet.

Det bör också nämnas att Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter medför behov av vissa ytterligare justeringar i det immaterialrättsliga sanktionssystemet. I

samband med genomförandet av detta direktiv kommer även vissa andra delar av sanktionssystemet att ses över.

6.6.4 Behovet av åtgärder

I fråga om brott mot upphovsrätt kan det konstateras att Sverige antingen redan har straffbestämmelser och andra sanktionsmöjligheter som uppfyller kraven i artiklarna 10 och 11 punkt 2 eller att det pågår lagstiftningsarbete för att införa sådana. Det bör anmärkas att det är underförstått att, om WIPO-fördragen ännu inte har trätt i kraft i förhållande till en viss stat, konventionen om IT-relaterad brottslighet inte ställer krav på särskild kriminalisering i avvaktan på att WIPO-fördragen träder i kraft (förklarande rapporten punkt 111). Några ändringar i reglerna om upphovsrätt krävs därför inte i detta sammanhang.

6.7 Försök och förberedelse till brott samt missbruk av hjälpmedel (artikel 6 och del av artikel 11)

Bedömning: Den nuvarande lagstiftningen uppfyller i allt väsentligt konventionens krav på straffansvar för osjälvständiga brottsformer. Försök till ringa brott är dock inte straffbelagt vid alla gärningar som enligt artikel 11 skall vara kriminaliserade på försöksstadiet. Reglerna om förberedelse innebär att det inte krävs någon särskild straffbestämmelse om missbruk av hjälpmedel.

6.7.1 Försök

Har någon påbörjat utförandet av ett brott utan att detta har kommit till fullbordan, skall han i de fall där det finns en särskild bestämmelse om detta, dömas för försök till brottet (23 kap. 1 § BrB). En förutsättning för ansvar är dock att det har funnits fara för brottets fullbordan eller att sådan fara har varit utesluten en-

dast på grund av tillfälliga omständigheter. Vidare döms inte till ansvar om gärningsmannen frivilligt avbrutit gärningen eller på annat sätt föranlett att brottet inte fullbordades. Straffet för försök skall bestämmas högst till vad som gäller för fullbordat brott och får inte sättas under fängelse om lägsta straff för det fullbordade brottet är fängelse i två år eller däröver.

Enligt artikel 11 punkt 2 skall försök till brott enligt artiklarna 3 (olovlig avlyssning av datorsystem), 4 (datastörning), 5 (systemstörning), 7 (dataförfalskning) 8 (databedrägeri) samt del av artikel 9 (framställning, spridning och överföring av barnpornografi) kriminaliseras.

Som redan har framgått finns det i de flesta fall regler om ansvar för försök i den utsträckning som behövs för att uppfylla kraven i artikel 11.

I vissa fall sträcker sig dock straffansvaret inte så långt att även försök till ringa brott är kriminaliserat. Frågan om Sverige bör begära undantag för vissa ringa brott behandlas i avsnitt 11.11.2.

6.7.2 Förberedelse till brott

Enligt 23 kap. 2 § BrB skall dömas för förberedelse till brott om någon, med uppsåt att utföra eller främja brott,
1. tar emot eller lämnar pengar eller annat som betalning för ett brott eller för att täcka kostnader för utförandet av ett brott eller
2. skaffar, tillverkar, lämnar, tar emot, förvarar, transporterar, sammanställer eller tar annan liknande befattning med något som är särskilt ägnat att användas som hjälpmedel vid ett brott,
under förutsättning att straffansvar för förberedelse är föreskrivet för brottet och att han inte har gjort sig skyldig till fullbordat brott eller försök.

I de fall där det särskilt anges döms för stämpling till brott. Med stämpling förstås att någon i samråd med annan beslutar gärningen eller att någon söker anstifta annan eller åtar sig eller erbjuder sig att utföra den.

Om faran för att brottet skulle fullbordas var ringa skall inte dömas till ansvar för förberedelse.

Reglerna om förberedelse till brott ändrades den 1 juli 2001. Straffansvaret utvidgades, samtidigt som bestämmelsen om förberedelse till brott gavs en mera generell utformning. Detta innebar att den tidigare kasuistiska uppräkningen av föremål som ansågs särskilt ägnade att användas som hjälpmedel vid brott ersattes med en allmän formulering, nämligen ”något som är särskilt ägnat att användas som hjälpmedel vid brott”.

I motiven till förändringen framhölls bl.a. att det var nödvändigt att modernisera straffansvaret för befattning med sådant som är ägnat att användas som hjälpmedel vid ett brott. Numera är således inte bara befattning med fysiska föremål utan även med immateriella objekt straffbar som förberedelse. Som exempel på det senare nämns i motiven datavirus och annan programvara som är framställd uteslutande i syfte att begå dataintrång eller andra typer av brott som t.ex. förfalskning (prop. 2000/01:85 s. 41).

Straffet för förberedelse och stämpling skall bestämmas under den högsta och får sättas under den lägsta straffnivå som gäller för fullbordat brott.

Artikel 6 förutsätter en omfattande kriminalisering av befattning med olika typer av hjälpmedel, från tekniska hjälpmedel och programvaror som är särskilt anpassade för att användas för de brott som behandlas i konventionen till datorlösenord, åtkomstkoder och liknande uppgifter. De sistnämnda är avsedda att enbart ha ett legalt användningsområde men kan, om de kommer i orätta händer, användas för att begå brott.

När det gäller hjälpmedel av förstnämnda slag anpassades, genom ändringen år 2001, den straffrättsliga lagstiftningen till den tekniska utvecklingen så att den täcker dessa.

Det är i förstone mera tveksamt om lösenord, åtkomstkoder och liknande kan betraktas som något som är särskilt ägnat att användas som ett hjälpmedel vid brott. Dessa har i huvudsak en legal användning. Eftersom de ingår i säkerhetsarrangemangen kring datoranläggningen eller datorsystemet har de emellertid en mycket viktig funktion och kan närmas jämföras med nycklar.

Åtkomstkoden och lösenordet är nyckeln till datorn i sig och till den lagrade informationen.

En vanlig nyckel är i sig inget hjälpmedel vid brott men den kan användas för tillträde till ett låst utrymme och för att tillgripa de fysiska föremål som finns där. Regeln om förberedelse har sedan länge tillämpats bl.a. på huvudnycklar och större uppsättningar av nycklar eftersom dessas funktion är att endast ge behöriga personer tillträde. I förberedelseparagrafens tidigare lydelse ingick dyrk i uppräkningen av föremål som ansågs särskilt ägnade som hjälpmedel för brott. Nycklar hänfördes under beteckningen ”annat sådant hjälpmedel”. Den som ertappades med t.ex. huvudnycklar till ett bostadsområde eller hotell eller med nycklar till lokaler eller bostäder som innehavaren saknade anknytning till kunde ådra sig ansvar för förberedelse till stöldbrott (jfr NJA 1960 s. 442).

Vid utvidgningen av straffansvaret för förberedelse framhöll regeringen att, för att ett hjälpmedel skall anses vara särskilt ägnat att användas som hjälpmedel vid brott, det bör krävas att det med hänsyn till sin beskaffenhet är av någorlunda central betydelse för brottet.

Det ter sig mot denna bakgrund naturligt att betrakta åtkomstkoder, datorlösenord och liknande uppgifter som är till för att skydda IT-miljöer mot obehöriga som något som i orätta händer är särskilt ägnat att användas som hjälpmedel för brott. Uppgifter av detta slag är ofta en grundläggande förutsättning för intrång i informationssystem.

Att utan lov ta befattning med, t.ex. avsiktligen sprida eller på annat sätt tillgängliggöra lösenord och åtkomstkoder, får därför anses falla in under regeln om förberedelse. Som tidigare påpekats är förberedelse till dataintrång straffbar, om det fullbordade brottet inte skulle ha varit att anse som ringa. Kraven i artikel 6 är därmed uppfyllda. Någon särskild straffregel som tar sikte på missbruk av hjälpmedel behövs därför inte. Frågan om straffansvar för förberedelse till ringa dataintrång måste däremot övervägas.

6.8 Medhjälp (del av artikel 11)

Bedömning: De befintliga reglerna om medhjälp uppfyller konventionens krav.

Enligt 23 kap. 4 § BrB skall straffansvar ådömas inte bara den som utfört gärningen utan även annan som har främjat denna med råd och dåd. Medverkansansvaret omfattar dels samtliga brott i brottsbalken dels straffbestämmelser i andra lagar och författningar under förutsättning att fängelse är föreskrivet för brottet.

Den som inte är att anse som gärningsman döms för anstiftan om han har förmått annan att utföra brottet. I övriga fall döms för medhjälp till brottet.

Varje medverkande skall bedömas efter det uppsåt eller den oaktsamhet som han har visat. Även i de fall brottet har ett s.k. specialsubjekt kan dömas för medverkan.

Den generella regleringen i 23 kap. BrB av medhjälp täcker de krav som ställs i detta hänseende i artikel 11 punkt 1.

6.9 Ansvar för juridiska personer (artikel 12)

Bedömning: Den nuvarande lagstiftningen uppfyller kraven i fråga om ansvar för juridiska personer.

6.9.1 Nuvarande regler

Enligt svensk rätt kan juridiska personer inte dömas till straffansvar. Däremot kan de åläggas ekonomiska sanktioner.

För brott som har begåtts i utövningen av näringsverksamhet kan näringsidkaren på yrkande av åklagaren åläggas företagsbot. Reglerna om företagsbot finns i 36 kap. BrB. Förutsättningarna för att ålägga någon företagsbot är dels att brottsligheten har inneburit ett grovt åsidosättande av de särskilda skyldigheter som är förenade med verksamheten eller annars är av allvarligt

slag, dels att näringsidkaren inte har gjort vad som skäligen kunnat krävas för att förebygga brottsligheten (36 kap. 7 § BrB). Om brottsligheten har varit riktad mot näringsidkaren eller om det annars skulle vara uppenbart oskäligt skall företagsbot inte åläggas.

En företagsbot skall vara lägst 10 000 kronor och högst tre miljoner kronor (36 kap. 8 § BrB). Företagsbot kan i vissa fall efterges eller sättas lägre. När storleken av företagsboten bestäms skall särskild hänsyn tas till brottslighetens art, omfattning och förhållande till näringsverksamheten.

Vidare finns det en särskild möjlighet att enligt 36 kap. 4 § BrB förverka ekonomiska fördelar som uppkommit för näringsidkare vid brott i näringsverksamhet, om inte förverkande skulle vara oskäligt. Vid denna bedömning skall bl.a. beaktas om det finns anledning att anta att annan betalningsskyldighet som svarar mot de ekonomiska fördelarna av brottet kommer att åläggas näringsidkaren eller annars fullgöras av denne.

6.9.2 Förslag till ändringar

Företagsbotsutredningen avgav år 1977 ett betänkande, Straffansvar för juridiska personer (SOU 1997:127), i vilket föreslogs att systemet med företagsbot skulle ersättas med ett helt nytt system med straffansvar för juridiska personer. Under remissbehandlingen av betänkandet riktades kritik mot att det inte hade utretts om det i stället var möjligt att effektivisera det nuvarande systemet. För att få underlag att bedöma den frågan har det inom Justitiedepartementet utarbetats en promemoria med förslag till sådana ändringar (Ds 2001:69; Företagsbot). Även promemorian har remissbehandlats. Regeringen har ännu inte tagit ställning till förslagen.

6.9.3 Behovet av åtgärder

I tidigare lagstiftningsärenden där frågan om ansvar för juridiska personer har varit aktuell (se t.ex. prop. 2003/04:70 s. 22) har regeringen och riksdagen gjort den bedömningen att reglerna om företagsbot uppfyller krav av det slag som ställs i den nu aktuella konventionen. De nuvarande reglerna om företagsbot och om förverkande av vinning får därför anses uppfylla kraven i artikel 12.

6.10 Påföljder m.m. (artikel 13)

Bedömning: Svensk rätt uppfyller kraven i konventionen på hur påföljderna skall var utformade.

Konventionen förutsätter att de brott som straffbeläggs i enlighet med artiklarna 2-11 bestraffas med effektiva, proportionella och avskräckande påföljder. Några konkreta krav på hur påföljderna skall var utformade ställs dock inte.

De straffskalor som gäller för nu aktuella brott har redovisats i det föregående. Dessa får anses uppfylla kraven i konventionen.

På motsvarande sätt uppfyller det nuvarande systemet för ansvar för ansvar för juridiska personer kraven i artikel 13.

6.11 Domsrätt (artikel 22)

Bedömning: Svensk lagstiftning uppfyller kraven i konventionen i fråga om regler om domsrätt.

6.11.1 Nuvarande regler

I 2 kap. BrB finns regler om tillämpligheten av svensk lag. Enligt 2 kap. 1 § BrB omfattar den svenska domsrätten alla brott som har begåtts på svenskt territorium, samt brott som det finns skäl

att anta har begåtts inom riket. Vidare omfattar den brott som svenska medborgare och utlänningar med hemvist i Sverige har begått utomlands, om det föreligger dubbel straffbarhet (2 kap. 2 § första stycket 1 BrB). Undantag har dock gjorts för brott som har begåtts inom område som inte tillhör någon stat, om det för brottet enligt svensk lag inte kan följa svårare straff än böter. Svensk domsrätt tillämpas vidare, under de förutsättningar som nyss har angetts, på bl.a. utlänning utan hemvist i Sverige som efter brottet har blivit svensk medborgare eller tagit hemvist här samt på medborgare i annat nordiskt land som vistas i Sverige (2 kap. 2 § första stycket 2).

Brott ombord på ett svenskt fartyg eller luftfartyg omfattas av svensk domsrätt enligt 2 kap. 3 § första stycket 1 BrB. Brott som inte har begåtts på någon stats territorium omfattas även i andra fall än som nyss har sagts av svensk domsrätt enligt 2 kap. 3 § första stycket 5, men endast om brottet har förövats mot en svensk medborgare, svensk sammanslutning eller enskild inrättning eller mot utlänning med hemvist i Sverige.

6.11.2 Förslag till ändringar

Reglerna i 2 kap. BrB om domsrätt har nyligen setts över av Internationella straffrättsutredningen (Internationella brott och svensk jurisdiktion; SOU 2002:98). Utredningen har lagt fram förslag till helt ny lydelse av 2 kap. BrB, eftersom de nuvarande reglerna anses svåröverskådliga. Betänkandet har remissbehandlats och bereds för närvarande i Justitiedepartementet.

Förslagen innebär i sak inga förändringar som har betydelse för detta lagstiftningsärende.

6.11.3 Behovet av åtgärder

De nuvarande reglerna om svensk domsrätt uppfyller de krav som ställs i artikel 22. Det behövs därför inga ändringar i reg-

lerna om domsrätt för att Sverige skall uppfylla åtagandena i konventionen.

6.12 De processrättsliga reglerna m.m.

6.12.1 Allmänt om de processrättsliga reglerna (artiklarna 14 och 15)

Bedömning: Rättegångsbalkens regler uppfyller generellt kraven i artiklarna 14 och 15 på rättssäkerhetsgarantier. Även kravet på oberoende tillsyn är uppfyllt.

De tvångsåtgärder av skilda slag som enligt konventionen skall kunna tillämpas motsvaras till stor del av regler i rättegångsbalken om straffprocessuella tvångsmedel. De tvångsmedel som framför allt kan aktualiseras är beslag, husrannsakan, hemlig teleavlyssning och hemlig teleövervakning. Även edition och företeende av föremål kan komma i fråga.

För att kraven i artikel 14 skall uppfyllas fordras det emellertid också att tvångsmedlen kan användas för de typer av brott som anges i konventionens artiklar 2-11. I de flesta fall är möjligheten att besluta om tvångsmedel knuten dels till en viss nivå på brottsmisstanken, dels till brottets straffskala. Härutöver kan det finnas andra krav. I det följande diskuteras dels om de befintliga tvångsmedlen är tillämpliga dels om de i något avseende behöver anpassas.

Rättegångsbalkens regler om straffprocessuella tvångsmedel uppfyller generellt kraven på rättssäkerhetsgarantier i artiklarna 14 och 15. Kravet på oberoende tillsyn är tillgodosett genom utformningen av Justitiekanslerns (JK) och Riksdagens ombudsmäns (JO) uppdrag.

6.12.2 Skyldighet att säkra information och att lämna uppgifter (artikel 16 och del av artikel 19)

Bedömning: Det finns inte någon regel som motsvarar kraven i artikel 19 punkt 4, som innebär att den som har kännedom om ett visst datorsystem, eller om säkerheten kring detta, skall kunna åläggas att lämna uppgifter härom. Det finns inte heller, utöver reglerna om hemliga tvångsmedel på teleområdet, någon regel som motsvarar kraven i artikel 16 på att enskilda skall kunna åläggas att temporärt bevara lagrad datainformation. Anpassningen till dessa artiklar kräver därför lagstiftningsåtgärder.

Alla som kan antas ha upplysningar av betydelse för utredningen är utan undantag skyldiga att låta sig förhöras under en förundersökning (23 kap. 6 § RB). Däremot finns det ingen skyldighet, vare sig för vittnen, målsägande eller misstänkt, att uttala sig under ett polisförhör. Den som uttalar sig har inte heller någon sanningsplikt. Den nuvarande regleringen ger inte utrymme för att, i enlighet med artikel 19 punkt 4, ålägga någon som har kännedom om ett datorsystem, eller om säkerheten kring detta, att lämna uppgifter som underlättar verkställigheten av tvångsmedel.

Ett av de från brottsutredningssynpunkt viktigaste inslagen i konventionen är kravet i artikel 16 på att en person skall kunna åläggas att temporärt bevara lagrade datorbehandlingsbara uppgifter som han innehar eller har kontroll över. Någon sådan skyldighet finns inte i svensk rätt, utöver vad som gäller i fråga om teleoperatörers skyldigheter att verkställa hemliga tvångsmedel på teleområdet. Reglerna om edition rör endast skyldigheten att lämna ut existerande handlingar och kan dessutom i liten utsträckning användas i brottmål (se avsnitt 6.12.5). Det krävs därför lagstiftning för att uppfylla kraven i artikel 16.

6.12.3 Beslag (del av artikel 19)

Bedömning: Reglerna om beslag uppfyller i de flesta hänseenden de krav som ställs i konventionen. Det krävs dock viss anpassning av beslagsreglerna till användning i IT-miljö om de i alla delar skall uppfylla åtagandena i artikel 19. Detta beror bl.a. på att de nuvarande reglerna förutsätter att beslag dels skall avse föremål, dels endast får läggas på föremål som är tillgängliga.

Nuvarande bestämmelser

Enligt 27 kap. 1 § RB får bl.a. föremål, som skäligen kan antas ha betydelse för utredning om brott eller kunna på grund av brott förverkas, tas i beslag.

Det är således inte någon förutsättning för beslag att det finns en misstänkt person. Inte heller uppställs det krav på att brottet skall vara av viss svårhetsgrad, med några nedan angivna undantag. Beslag kan därför förekomma vid alla typer av brott och riktas mot såväl misstänkta som andra. Beslag får dock beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse.

Beslag får även läggas på skriftlig handling (27 kap. 2 § RB). Det har från tid till annan diskuterats i vilken utsträckning digitalt lagrad information kan sägas falla under begreppet handling (se bl.a. prop. 1998/99:11 s. 54 f och Ds 2003:29 s. 95 f). I praxis jämställs i RB i många avseenden en urskiljbar elektronisk handling (dvs. en viss avgränsad sammanställning av elektroniska data) med en skriftlig handling. Framställningssättet saknar betydelse för reglerna om beslag. Däremot är det av avgörande betydelse om den elektroniska informationen har fixerats på ett fysiskt medium eller ej. Vad som är viktigt i detta sammanhang är nämligen att regleringen i RB utgår från att en handling har fysisk form eftersom beslagsinstitutet inte kan tillämpas på immateriella objekt. Det är osäkert om data i elektronisk form som

inte har sammanställts kan anses motsvara en skriftlig handling och således kan tas i beslag. Det finns även andra problem förknippade med att lagstiftningen om beslag utgår från att handlingar har fysisk form (se avsnitt 11.6).

En skriftlig handling får inte tas i beslag om innehållet i handlingen är sådant att någon som räknas upp i 36 kap. 5 § RB inte får höras som vittne om innehållet och handlingen innehas antingen av honom eller av den till vars förmån tystnadsplikten gäller (27 kap. 2 § RB).

Hos den misstänkte eller hans närstående får beslag läggas på skriftlig handling mellan honom och hans närstående eller mellan hans närstående inbördes, men endast om det för brottet inte är föreskrivet lindrigare straff än fängelse två år.

Beslag av brev eller annan försändelse hos ett befordringsföretag förutsätter att det är föreskrivet fängelse ett år eller mer för brottet (27 kap. 3 § RB). Vidare krävs det att försändelsen hade kunnat tas i beslag hos mottagaren. Elektronisk post faller dock utanför bestämmelsens tillämpningsområde. För elektronisk post gäller i stället reglerna om hemlig teleavlyssning och hemlig teleövervakning samt bestämmelserna i lagen (2003:398) om elektronisk kommunikation, eftersom elektronisk post lagtekniskt är ett telemeddelande.

En förutsättning för att något skall kunna tas i beslag är att föremålet i fråga påträffas, dvs. är tillgängligt. Reglerna om husrannsakan ger myndigheterna en möjlighet att söka efter föremål som kan komma att tas i beslag. Förutsättningarna för beslut om husrannsakan är dock strängare än förutsättningarna för beslag.

Ett elektroniskt meddelande som har överförts till papper eller materialiserats i annan fysisk form är, med det undantag som anges nedan, åtkomligt för beslag enligt vanliga regler. Likaså kan ett elektroniskt meddelande som finns lagrat i en dator hos någon annan än en teleoperatör, t.ex. hos abonnenten, tas i beslag, om förutsättningarna i övrigt är uppfyllda.

Hos en teleoperatör får beslag inte användas som substitut för hemlig teleövervakning. Hemlig teleövervakning reglerar exklusivt möjligheterna att hos en teleoperatör med straffprocessuella

tvångsmedel få fram uppgifter om teletrafik och annan elektronisk kommunikation. Detta anses följa av de allmänna principerna om dels lex specialis (dvs. att en lag som reglerar ett speciellt förhållande äger företräde framför en lag av allmän karaktär), dels lex posterior (dvs. att senare tillkommen lag tar över äldre lag). Se JO 1997/98 s. 47 ff., SOU 1998:46 s. 371 ff och prop. 2002/03:74 s. 45 f. Det finns emellertid, som utvecklas närmare i det följande, även bestämmelser i lagen om elektronisk kommunikation om skyldighet för teleoperatörer att lämna vissa uppgifter till brottsbekämpande myndigheter.

Även om uppgifter om elektronisk kommunikation finns tillgängliga hos en operatör i sådan form att beslag skulle vara möjligt får dessa således inte tas i beslag hos denne.

Det är inte helt ovanligt att delar av beslag kan behöva användas som bevisning såväl vid en rättegång i Sverige som i förundersökning eller rättegång utomlands. Utan hinder av att beslaget består kan föremål eller handlingar lånas ut för att användas i ett rättsligt förfarande i en annan stat. En förutsättning för att beslag skall kunna lånas ut är dock att det från svensk sida ställs upp villkor att det beslagtagna skall återställas inom viss kortare tid (se NJA 1990 s. 635).

Förslag till ändringar

Datastraffrättsutredningen föreslog i sitt betänkande (SOU 1992:110) bl.a. att reglerna om beslag skulle anpassas till modern teknisk miljö. Förslaget innebar borttagande av kravet på att en handling skall vara skriftlig för att den skall kunna tas i beslag. Genom att använda begreppet handling för såväl traditionella skriftliga handlingar som elektroniska dokument tillgodosågs enligt utredningen kraven på anpassning till modern teknik. Betänkandet, som har remissbehandlats men inte lett till någon lagstiftning, anses numera vara obsolet i stora delar.

Polisrättsutredningen lade i sitt slutbetänkande (SOU 1995:47; Tvångsmedel enligt 27 och 28 kap. RB samt polislagen) fram förslag till ändrad lydelse av flertalet regler om beslag. De

grundläggande reglerna om beslag skulle enligt förslaget i princip vara oförändrade, men omarbetades. De sakliga förändringar som utredningen föreslog berörde främst beslutsbehörigheten och verkställigheten. De saknar därför betydelse för detta lagstiftningsärende. Förslagen övervägs inom Justitiedepartementet.

Behovet av åtgärder

Reglerna om beslag uppfyller i de flesta hänseenden kraven i artikel 19. Reglerna måste emellertid anpassas bättre till användning i IT-miljö om de i alla delar skall uppfylla åtagandena i konventionen, eftersom dessa förutsätter att även sådana datorbehandlingsbara uppgifter som inte är fixerade vid ett fysiskt medium skall kunna tas i beslag. Vidare måste frågan om tillåtligheten av kopiering av beslag övervägas.

Det bör också i fråga om artikel 19 punkt 3 d noteras att beslag i dessa fall endast utgör förstadiet till det beslut om förverkande som torde krävas. Framtida förverkande är en av de grunder som får användas för beslag. Den generella utformningen av förverkandereglerna i 36 kap. BrB innebär att det finns tillräckligt utrymme för att använda beslag för att säkra framtida förverkande.

6.12.4 Husrannsakan (del av artikel 19)

Bedömning: Reglerna om husrannsakan uppfyller till största delen de krav som ställs i konventionen. Det krävs dock viss anpassning för att Sverige helt skall uppfylla kraven i artikel 19.

Nuvarande bestämmelser

Om det förekommer anledning att ett brott, på vilket fängelse kan följa, har förövats, får husrannsakan företas i hus, rum eller

slutet förvaringsställe antingen för att söka efter föremål som är underkastat beslag eller för att utröna omständighet som kan ha betydelse för utredning om brottet (28 kap. 1 § RB).

För husrannsakan hos den misstänkte krävs att denne är skäligen misstänkt. Husrannsakan får företas även hos annan än den som är skäligen misstänkt, men då krävs det att det finns synnerlig anledning att anta att det genom husrannsakan skall påträffas föremål som skall tas i beslag eller att annan utredning om brottet kan vinnas. Husrannsakan hos annan får även företas om brottet har förövats där eller om den misstänkte har gripits där.

Husrannsakan kan äga rum såväl i bostäder som på arbetsplatser och andra ställen. Några begränsningar i fråga om vilka lokaler som får genomsökas finns inte. Husrannsakan kan således, om förutsättningarna i övrigt är uppfyllda, göras var helst det finns en dator eller annan teknisk utrustning som kan antas ha använts för brott. Den tidigare nämnda bestämmelsen i 27 kap. 2 § RB om beslagsförbud får emellertid indirekt betydelse för frågan om husrannsakan är möjlig. Är det inte tillåtet att ta ett föremål eller en handling i beslag får inte husrannsakan genomföras för att söka efter objektet i fråga (NJA 1977 s. 403).

I en lokal som är tillgänglig för allmänheten får husrannsakan företas för de ändamål som nyss har sagts även om det inte finns någon som är skäligen misstänkt och oberoende av brottets svårhetsgrad (28 kap. 3 § första stycket RB). Med lokal som är tillgänglig för allmänheten avses bl.a. butiker, restauranger, kaféer, teater- och biograflokaler. Ett internetcafé som är öppet för allmänheten torde höra till de lokaler där bestämmelsen kan tillämpas.

I en lokal som brukar användas gemensamt av personer som kan antas ägna sig åt brottslig verksamhet får också husrannsakan företas för de ändamål som nyss har angetts. Förutsättningarna är att det förekommer anledning att brott med fängelse ett år eller mera i straffskalan har förövats och att det finns särskild anledning att anta att ändamålet med rannsakningen kommer att uppfyllas (28 kap. 3 § andra stycket RB). Rätten att genomföra sådan husrannsakan omfattar också utrymmen och fordon som

finns i omedelbar anslutning till lokalen och som brukas av dem som använder lokalen.

För husrannsakan gäller samma allmänna begränsning som för beslag, nämligen att husrannsakan får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse (28 kap. 3 a § RB).

Under en husrannsakan kan det bli aktuellt att genomsöka en dator för att finna elektroniska dokument, filer eller spår av kommunikation. Det finns inga särregler om undersökning av datorer. Vad som bör observeras är dock att en sådan undersökning kan, till följd av den tekniska utvecklingen, komma att beröra ett annat land. Om nämligen datorn är uppkopplad till en server som finns utomlands anses det att en undersökning av det som är tillgängligt i datorn via servern utgör en husrannsakan utomlands.

I prop. 2002/03:74 har framhållits att det inte är rättsenligt att genom husrannsakan skaffa fram sådana uppgifter från en teleoperatör som omfattas av reglerna om hemlig teleavlyssning eller hemlig teleövervakning (s. 45 f). Dessa tvångsmedel reglerar, som nyss har nämnts, exklusivt åtkomsten av uppgifter om innehållet i ett telemeddelande eller uppgifter om teletrafik.

Förslag till ändringar

Datastraffrättsutredningen föreslog i sitt betänkande bl.a. att reglerna om husrannsakan skulle anpassas till modern teknisk miljö. Betänkandet, som har remissbehandlats men inte lett till någon lagstiftning, anses numera vara obsolet i stora delar. Förslaget om nya regler för husrannsakan i datormiljö redovisas närmare i avsnitt 11.6.3.

Polisrättsutredningen lade i sitt slutbetänkande (se avsnitt 6.12.3) fram förslag till omfattande förändringar av 28 kap. RB. Utredningen föreslog bl.a. att begreppet husrannsakan skulle utmönstras och att de nuvarande reglerna om husrannsakan skulle ersättas med nya regler om undersökning av mer integri-

tetskänsliga respektive mindre integritetskänsliga utrymmen. Ändringarna, som i sak inte var särskilt stora, innebar främst en språklig modernisering och en omarbetning av kapitlet. Betänkandet har remissbehandlats. Förslagen övervägs inom Justitiedepartementet.

Behovet av åtgärder

Reglerna om husrannsakan uppfyller i många hänseenden de krav som ställs i konventionens artikel 19. Av samma skäl som reglerna om beslag måste anpassas bättre till IT-miljön krävs det dock vissa ändringar i reglerna om husrannsakan eftersom dessa enbart tar sikte på undersökning av en fysisk miljö. Vidare måste frågan om de nuvarande möjligheterna till utvidgad husrannsakan är tillräckliga samt om man bör införa en möjlighet till husrannsakan via kommunikationsnät övervägas.

6.12.5 Edition (del av artikel 18)

Bedömning: Reglerna om edition har liten betydelse för anpassningen till konventionen. Eftersom edition endast i mycket begränsad omfattning kan användas i brottmål finns det inget egentligt behov av att ändra editionsreglerna, annat än om det är fråga om konsekvensändringar.

Den som innehar en skriftlig handling, som kan antas ha betydelse som bevis, är enligt 38 kap. 2 § RB skyldig att förete den (s.k. editionsskyldighet). Högsta domstolen har inte ansett hinder möta mot att utfärda editionsföreläggande beträffande elektroniskt lagrad information som kräver särskild bearbetning för ta fram materialet i läsbar form (NJA 1998 s. 829).

I brottmål är dock den misstänkte undantagen från editionsskyldighet och likaså hans närstående. Editionsskyldigheten ersätts i brottmål av de nyss redovisade reglerna om beslag och husrannsakan. Vidare har från editionsskyldigheten gjorts mot-

svarande undantag som finns i regeln om beslagsförbud för handlingar vilkas innehåll är sådant att det omfattas av tystnadsplikt som inte bryts av skyldigheten att vittna. Det finns även vissa andra undantag från editionsskyldigheten.

Dessutom kan föreläggande om edition över huvud taget inte utfärdas i fall där det inte finns någon som är skäligen misstänkt (NJA 2003 s. 107). Detta innebär att edition aldrig kan användas i det inledande stadiet av en brottsutredning.

En annan viktig begränsning i detta sammanhang är att reglerna om editionsföreläggande, i likhet med reglerna om beslag och husrannsakan, inte får användas för att tvinga fram sådana uppgifter hos en teleoperatör som omfattas av reglerna om hemlig teleavlyssning och hemlig teleövervakning (prop. 2002/03:74 s. 45 f).

Nu nämnda inskränkningar i tillämpningsområdet innebär att reglerna om edition har mycket begränsad betydelse för anpassningen till konventionen.

Bestämmelserna om edition har betydelse framför allt för kraven i artikel 18. Reglerna om edition uppfyller formellt kraven i konventionens artikel 18 punkt 1 a. Något behov av att ändra reglerna finns därför inte, utom för det fall att det krävs konsekvensändringar av något slag.

Den begränsade faktiska möjligheten att använda edition i brottmål innebär emellertid att det i stället är reglerna om husrannsakan och beslag som är centrala för frågan om Sverige uppfyller åtagandena i artikel 18 punkt 1 a. Som redan har framgått krävs det vissa ändringar i dessa regler.

6.12.6 Hemlig teleavlyssning och hemlig teleövervakning (artiklarna 20 och 21)

Bedömning: Reglerna om hemlig teleavlyssning uppfyller de grundläggande kraven på att tvångsmedlet kan användas vid grova brott. Det nuvarande undantaget för avlyssning i telenät av mindre betydelse från kommunikationssynpunkt torde dock vara alltför omfattande för att uppfylla konventionens

krav. Samma undantag gäller för hemlig teleövervakning. Det krävs således vissa lagstiftningsåtgärder för att uppfylla kraven i artiklarna 20 och 21.

Nuvarande bestämmelser

Kommunikation mellan datorer kan avlyssnas med stöd av reglerna i 27 kap. RB om hemlig teleavlyssning. Hemlig teleavlyssning innebär att telemeddelanden som befordras till eller från en teleadress i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet. Med telemeddelande avses enligt 6 kap. 19 § tredje stycket lagen om elektronisk kommunikation ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.

Hemlig teleavlyssning får användas vid förundersökning angående dels brott för vilket inte är föreskrivet lindrigare straff än fängelse två år, dels vid försök, förberedelse eller stämpling till sådant brott, om gärningen är belagd med straff (27 kap. 18 § RB). Den 1 oktober 2004 utvidgades tillämpningsområdet på det sättet att hemlig teleavlyssning numera också får användas vid brott som har ett straffvärde som kan antas överstiga två års fängelse (prop. 2002/03:74).

Uppgifter om telemeddelanden som har expedierats eller beställts till eller från en viss teleadress kan vidare hämtas in med stöd av reglerna om hemlig teleövervakning (27 kap. 19 § RB). Hemlig teleövervakning får inte avse innehållet i meddelandena utan enbart trafiken i sig. Hemlig teleövervakning får användas vid förundersökning angående brott för vilket inte är föreskrivet lindrigare straff än sex månaders fängelse. Vidare får hemlig teleövervakning användas vid några brottstyper som räknas upp i en särskild brottskatalog. Den 1 oktober 2004 utökades katalogen med två brott som är av särskilt intresse i detta sammanhang, nämligen dataintrång och barnpornografibrott.

Dessutom får hemlig teleövervakning användas vid förundersökning angående försök, förberedelse och stämpling till brott för vilket inte är föreskrivet lindrigare straff än sex månaders fängelse. Vidare får hemlig teleövervakning avse även osjälvständiga brottsformer av de brott som anges i den särskilda brottskatalogen.

Hemlig teleavlyssning och hemlig teleövervakning får beslutas bara om någon är skäligen misstänkt och om åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § RB).

Åtgärden riktas i första hand mot en teleadress som innehas eller annars kan komma att användas av den misstänkte. Med teleadress avses ett telefonnummer, en enskild anknytning i en telefonväxel, en kod eller annan teleadress (exempelvis adressen för elektronisk post). Hemlig teleavlyssning och hemlig teleövervakning får, efter lagändringen den 1 oktober 2004, avse inte bara den teleadress från vilken den misstänkte ringer eller kommunicerar på annat sätt utan även en teleadress till vilken denne kan antas ringa eller sända ett telemeddelande.

Både hemlig teleavlyssning och hemlig teleövervakning får numera beslutas beträffande lagrade uppgifter om telemeddelanden i förfluten tid.

Beslut om hemlig teleavlyssning eller hemlig teleövervakning meddelas av domstol på ansökan av åklagare (27 kap. 21 § RB). En domstol kan således inte på eget initiativ ta upp en sådan fråga.

En åklagare får inte besluta interimistiskt om hemliga tvångsmedel på teleområdet, utom i fråga om sådana brott som avses i lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål (1952 års lag).[32] Den lagen är inte tillämplig på de brott som omfattas av konventionen, med undantag för om ett dataintrång skulle vara att bedöma som sabotage eller grovt sabotage.

En generell begränsning är att hemlig teleavlyssning och hemlig teleövervakning inte får avse telemeddelanden som endast

[32] Vid krig eller krigsfara har åklagaren också rätt att interimistiskt besluta om hemliga tvångsmedel, se 28 § lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara, m.m.

befordras inom ett telenät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt (27 kap. 20 § andra stycket RB). Frågan huruvida ett telenät skall anses vara av mindre betydelse eller inte skall avgöras utifrån en samlad bedömning av olika omständigheter som rör telenätets betydelse från allmän kommunikationssynpunkt (prop. 1994/95:227 s. 31). I ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning skall särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga telenät.

Hemlig teleavlyssning får inte omfatta telefonsamtal eller andra telemeddelanden mellan den misstänkte och hans försvarare (27 kap. 22 § RB).

I ärenden om hemlig teleavlyssning har nyligen införts ett system med offentliga ombud. Det offentliga ombudet har till uppgift att bevaka enskildas integritetsintressen i allmänhet. Ombudet företräder således inte den som är misstänkt eller som annars kan komma att drabbas av tvångsmedlet. Det offentliga ombudet har rätt att få tillgång till allt material som ligger till grund för domstolens prövning och har vidare rätt att yttra sig i ärendet och att överklaga domstolens beslut. Ett offentligt ombud får inte obehörigen avslöja vad han fått kännedom om genom uppdraget.

Om det inte längre finns skäl för ett beslut om hemlig teleavlyssning eller hemlig teleövervakning skall åklagaren eller rätten omedelbart häva beslutet (27 kap. 23 § RB).

Behovet av åtgärder

De nuvarande reglerna om hemliga tvångsmedel på teleområdet innebär att flertalet av de krav som ställs i konventionen är uppfyllda.

Bestämmelserna om hemlig teleavlyssning uppfyller i allt väsentligt kraven på regler om avlyssning i artikel 21. Som tidigare nämnts är det tillräckligt att det finns möjlighet att använda hemlig teleavlyssning för grova brott. Den närmare omfatt-

ningen av tillämpningsområdet bestäms i nationell rätt. Däremot är det tveksamt om det nuvarande undantaget för avlyssning av telenät av begränsad betydelse står i överensstämmelse med konventionens krav. Motsvarande undantag gäller för hemlig teleövervakning.

Tillämpningsområdet för hemlig teleövervakning torde inte helt uppfylla kraven i artikel 20. Tvångsmedlet kan nämligen inte användas för alla de brott som enligt artiklarna 2-11 skall vara kriminaliserade och det är inte heller tillåtet att använda andra tvångsmedel hos operatörer. Anpassningen till konventionen kräver således vissa lagstiftningsåtgärder.

6.12.7 Röjande av trafikuppgifter m.m. (artikel 17 och del av artikel 18)

Bedömning: De nuvarande reglerna i lagen om elektronisk kommunikation uppfyller inte kraven i artikel 17 på snabbt säkrande och röjande av trafikuppgifter. Inte heller reglerna om hemlig teleövervakning är tillräckliga för att uppfylla konventionsåtagandena. Även anpassningen till artikel 17 kräver därför lagstiftning. Däremot är bestämmelserna i lagen om elektronisk kommunikation om utlämnande av uppgifter om abonnemang tillräckliga.

Nuvarande bestämmelser

Lagen om elektronisk kommunikation innehåller, i likhet med den tidigare telelagen, regler om verkställighet av hemlig teleavlyssning och hemlig teleövervakning. Där regleras också operatörers tystnadsplikt och deras skyldighet att, utan hinder av tystnadsplikten, lämna uppgifter till bl.a. brottsbekämpande myndigheter.

I 6 kap. 19 § lagen om elektronisk kommunikation läggs fast vad som krävs av den som bedriver verksamhet där beslut om hemliga tvångsmedel kan komma att verkställas. Denne är skyl-

dig att bedriva verksamheten så att beslut om hemlig teleavlyssning eller hemlig teleövervakning kan verkställas och så att verkställandet inte röjs

Skyldigheten knyts inte längre till viss tillståndspliktig verksamhet utan till arten av verksamhet. Om det är fråga om verksamhet som anges i nedanstående två punkter måste kravet på att hemliga tvångsmedel skall kunna verkställas utan att tvångsmedelsanvändningen röjs uppfyllas;

1. ett allmänt kommunikationsnät som inte enbart är avsett för radioutsändning till allmänheten eller annat ändamål som anges i 1 kap. 1 § tredje stycket YGL eller
2. tjänster inom ett allmänt kommunikationsnät vilka består av

a/ en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation, som medger funktionell tillgång till Internet eller

b/ en allmänt tillgänglig elektronisk kommunikationstjänst till mobil anslutningspunkt.

Vidare skall innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden göras tillgängligt så att informationen enkelt kan tas om hand. Sistnämnda bestämmelse innebär ett krav på att uppgifterna skall ha sådan form att de kan avlyssnas eller läsas.

I 6 kap. 22 § lagen om elektronisk kommunikation föreskrivs i vilken utsträckning som den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst är skyldig att, trots tystnadsplikten, lämna uppgifter till bl.a. brottsbekämpande myndigheter. Angående tystnadspliktens omfattning se avsnitt 6.14.2.

Den som driver sådan verksamhet som nyss sagts är för det första skyldig att på begäran av en åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brott lämna uppgift om ett abonnemang som angår misstanke om brott. För att skyldigheten skall inträda krävs det att fängelse är föreskrivet för brottet och att detta enligt myndighetens bedömning kan föranleda annan påföljd än böter. Undantaget från

tystnadsplikten i fråga om uppgift om abonnemang omfattar exempelvis uppgift om namn, titel, adress på innehavaren av abonnemanget och telefonnummer.

För det andra är den som bedriver sådan verksamhet skyldig att på begäran av nyss nämnda myndigheter lämna annan uppgift som rör ett särskilt meddelande än innehållet i detta. I dessa fall ställs det strängare krav på brottet. Det krävs att det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, dvs. samma huvudkrav som gäller för beslut om hemlig teleavlyssning. De uppgifter som avses är enligt förarbetena t.ex. uppgift om mellan vilka teleadresser ett meddelande har utväxlats, samt datum och tidpunkt för meddelandet (prop. 1995/96:180 s. 13).

Uppgift om *innehållet* i ett elektroniskt meddelande får aldrig lämnas ut med stöd av reglerna i lagen om elektronisk kommunikation.

Bestämmelserna om tystnadsplikt och utlämnande har i sak oförändrade förts över från telelagen till den nya lagen om elektronisk kommunikation, men tillämpningsområdet har som framgått ovan utvidgats och omfattar numera även den som bedriver kommunikationstjänster av visst slag.

De nu beskrivna reglerna i lagen om elektronisk kommunikation innebär att dessa (i likhet med telelagens regler) och reglerna om hemlig teleövervakning delvis överlappar varandra.

Behovet av åtgärder

Genom regleringen i lagen om elektronisk kommunikation uppfylls åtagandena i artikel 18 punkt 1 b om utlämnande av abonnemangsuppgifter. Däremot uppfyller reglerna om röjande av uppgifter om ett telemeddelande inte de krav som ställs i artikel 17.

Reglerna om hemlig teleövervakning, som redovisats i föregående avsnitt, ger också möjlighet att inhämta trafikuppgifter. De nuvarande reglerna om hemlig teleövervakning är inte heller de tillräckliga för att uppfylla kravet i artikel 17 på snabbt röjande av trafikuppgifter. Detta beror bl.a. på att domstolsbeslut måste

hinna utverkas och på att tvångsmedlet endast får användas vid grövre brott.

Eftersom de nuvarande bestämmelserna inte är tillräckliga för att uppfylla kraven i artikel 17 på snabbt röjande av trafikuppgifter krävs det lagstiftningsåtgärder.

6.13 Internationellt samarbete

6.13.1 Internationell rättslig hjälp (artiklarna 23, 25, 27 och 29-35)

Bedömning: Reglerna om internationell rättslig hjälp uppfyller i allt väsentligt de krav som ställs i konventionen. Eftersom det inte finns några regler i svensk rätt som motsvarar kraven i artiklarna 16 och 17 om snabbt säkrande och röjande av lagrade datorbehandlingsbara uppgifter finns det inte heller regler som uppfyller kraven i artiklarna 29 och 30 på rättslig hjälp med sådana åtgärder. Det krävs därför lagstiftningsåtgärder som gör att de nya tvångsmedel som tillskapas som ett led i anpassningen till konventionen också får genomslag i lagstiftningen om rättslig hjälp. Detsamma gäller andra utredningsbefogenheter. Det finns för närvarande inte någon regel om uppskjutande av verkställighet enligt artikel 27 punkt 5, vilket kräver närmare överväganden.

Nuvarande bestämmelser

Något om utvecklingen av det internationella samarbetet

Utgångspunkten i konventionen om IT-relaterad brottslighet är att staterna skall ha en lagstiftning som i största möjliga utsträckning tillåter samarbete över gränserna. Artikel 27 om ömsesidig rättslig hjälp reglerar enbart rättslig hjälp i de fall där det inte finns någon lagstiftning eller bindande överenskommelse mellan staterna.

Trots att lagstiftningen om internationell rättslig hjälp är ganska ny är den föremål för förändringar. Utvecklingen av det internationella samarbetet i rättsliga frågor går nämligen mycket snabbt för närvarande, framför allt inom den Europeiska unionen. Det innebär att frågor av samma slag som behandlas i konventionen om IT-relaterad brottslighet är föremål för övervägande i andra sammanhang. En aktuell redovisning av internationella konventioner och överenskommelser som behandlar rättslig hjälp finns i Ds 2004:50 s. 53. I det följande redogörs kortfattat för sådana lagstiftningsärenden som har direkt beröring med anpassningen till konventionen om IT-relaterad brottslighet.

Nuvarande möjligheter till rättslig hjälp

Lagen (2000:562) om internationell rättslig hjälp reglerar rättsligt samarbete mellan åklagare och domstolar. Däremot faller internationellt polis- och tullsamarbete utanför regleringen. Lagen kan emellertid vara tillämplig om en utländsk polis- eller tullmyndighet begär rättslig hjälp t.ex. med husrannsakan. Om nämligen Sverige till följd av en bindande internationell överenskommelse godkänner att framställning om rättslig hjälp görs av en sådan myndighet behandlas framställningen som om den hade gjorts av åklagare eller domstol. Detta är en följd av att andra länder har organiserat den brottsutredande och brottsbeivrande verksamheten på annat sätt än vad som är fallet i vårt land.

Lagen omfattar inte rättslig hjälp beträffande brott som handläggs enligt reglerna i YGL och TF (prop. 1999/2000:61 s. 73).

Lagen bygger på principen att de åtgärder och tvångsmedel som får förekomma i en svensk förundersökning också kan beslutas på begäran av en främmande stat, i vissa fall dock med den begränsningen att det krävs dubbel straffbarhet.

Rättslig hjälp kan enligt 1 kap. 2 § lagen om internationell rättslig hjälp omfatta följande åtgärder:

1. förhör i samband med förundersökning i brottmål,
2. bevisupptagning vid domstol,
3. telefonförhör,

4. förhör genom videokonferens,
5. kvarstad, beslag samt husrannsakan och andra åtgärder som avses i 28 kap. RB,
6. hemlig teleavlyssning och hemlig teleövervakning,
7. hemlig kameraövervakning,
8. överförande av frihetsberövade för förhör och
9. rättsmedicinsk undersökning av avliden.

Lagen hindrar inte att hjälp lämnas med andra åtgärder om det kan ske utan tvångsmedel eller andra tvångsåtgärder.

När lagen om internationell rättslig hjälp tillskapades valde man avsiktligt att ge lagen ett vidare tillämpningsområde än vad som krävdes med hänsyn till då gällande internationella överenskommelser, t.ex. att låta den omfatta sådana tvångsmedel som hemlig teleavlyssning och hemlig teleövervakning. Syftet med detta var att för framtiden skapa största möjliga utrymme för internationellt samarbete, vilket står i god överensstämmelse med kraven i artikel 23.

Rättslig hjälp kan lämnas oberoende av om brottsutredningen riktar sig mot en fysisk eller en juridisk person (1 kap. 3 §). Vidare kan rättslig hjälp med de ovan uppräknade åtgärderna lämnas även i ärenden som i den ansökande staten eller i Sverige handläggs i ett administrativt förfarande eller ett annat förfarande än ett straffrättsligt sådant (1 kap. 5 §).

Det krävs dubbel straffbarhet såväl för ansökningar om husrannsakan och beslag som för ansökningar om bl.a. hemlig teleavlyssning och hemlig teleövervakning (2 kap. 2 §). När det gäller husrannsakan och beslag är kravet på dubbel straffbarhet uppmjukat i förhållande till vissa länder (4 kap. 20 §). En annan syn på kravet på dubbel straffbarhet kräver därför lagstiftningsåtgärder.

Möjligheterna att vägra rättslig hjälp är begränsade. I lagen om internationell rättslig hjälp finns det både obligatoriska och fakultativa vägransgrunder. En ansökan om rättslig hjälp skall avslås om ett bifall skulle kränka Sveriges suveränitet, medföra fara för rikets säkerhet eller strida mot svenska allmänna rättsprinciper eller andra väsentliga intressen (2 kap. 14 § första stycket).

En ansökan om rättslig hjälp får också avslås
1. om gärningen har karaktär av ett politiskt brott,
2. om gärningen utgör ett militärt brott, om inte gärningen motsvarar även annat brott som enligt svensk rätt inte är ett militärt brott,
3. om det i Sverige har meddelats dom eller beslut om åtalsunderlåtelse beträffande gärningen, eller
4. om omständigheterna annars är sådana att ansökan inte bör bifallas (2 kap. 14 § andra stycket). De nu nämnda grunderna för avslag gäller inte om ett avslag skulle strida mot en gällande internationell överenskommelse. En ansökan från en medlem inom den Europeiska unionen eller från en annan nordisk stat får inte heller avslås på den grunden att det är fråga om ett politiskt brott.

Enligt konventionen får som skäl för att vägra hjälp för det första åberopas att det är fråga om ett politiskt brott eller ett brott med anknytning till ett sådant brott (artikel 27 punkt 4 a). En annan grund för vägran är om verkställandet av framställningen kan komma att inkräkta på statens suveränitet, säkerhet, allmän ordning eller andra viktiga intressen (artikel 27 punkt 4 b). De obligatoriska grunderna för avslag har således täckning i konventionen. Eftersom den paragraf i lagen om internationell rättslig hjälp som behandlar fakultativa vägransgrunder har ett generellt undantag för den händelse det finns avvikande regler i en internationell överenskommelse är någon lagstiftningsåtgärd inte nödvändig.

Däremot finns det för närvarande inte någon regel som medger att verkställigheten av en framställning om rättslig hjälp skjuts upp av hänsyn till att verkställigheten kan skada pågående förundersökning och lagföring i Sverige (artikel 27 punkt 5).

Innehållet i artikel 32 bereder i sak inga problem ur svensk synvinkel i de delar den behandlar åtkomst till allmänt tillgänglig information. Att tillåta åtkomst till ett datorsystem i ett annat land, när åtkomsten har möjliggjorts genom ett lagenligt och frivilligt samtycke en person som har rätt att lämna ut informationen, torde inte heller kräva några lagstiftningsåtgärder, även

om samtycke till tvångsmedel inte generellt tillerkänns någon verkan i svensk rätt.

Reglerna i lagen om internationell rättslig hjälp uppfyller i princip kraven i artiklarna 31, 33 och 34 eftersom lagen medger hjälp med husrannsakan, beslag, hemlig teleövervakning och hemlig teleavlyssning. I fråga om hemlig teleavlyssning och hemlig teleövervakning ställer konventionen inte högre krav än att rättslig hjälp skall kunna ges för brott där tvångsmedlet hade kunnat användas i ett inhemskt förfarande.

Förfarandet

I lagen om internationell rättslig hjälp finns det också regler om förfarandet vid ansökan om och verkställighet av rättslig hjälp.

Lagen medger i princip användning av moderna kommunikationsmedel som telefax och elektronisk post vid ansökan och annan kommunikation. Vidare förutsätter lagen att direktkommunikation mellan myndigheter i Sverige och utlandet kommer att användas i allt större utsträckning. Regleringen står i god överensstämmelse med innehållet i artikel 25.

Inom Justitiedepartementet finns Centralmyndigheten för internationellt rättsligt samarbete (se prop. 1999/2000:61 s. 90 ff angående inrättandet). Centralmyndigheten tar emot, granskar och vidarebefordrar framställningar till och från Sverige bl.a. i ärenden om internationell rättslig hjälp och utlämning i de fall där inte direktkommunikation förekommer mellan den svenska och den utländska myndigheten. Centralmyndigheten lämnar också upplysningar till svenska och utländska myndigheter om innehållet i svensk och utländsk rätt samt har vidare till uppgift att ge service och råd till svenska och utländska myndigheter i fråga om internationellt rättsligt samarbete. Kravet i artikel 27 punkt 2 a på en centralmyndighet utgör således inget problem.

Enligt artikel 35 skall det finnas en kontaktpunkt som är tillgänglig dygnet runt året om för att ge hjälp och vägledning. Hjälpen skall bl.a. ta sikte på tekniska råd, rättslig information, lokalisering av misstänkta samt att kunna få till stånd skyndsamt

säkrande enligt artiklarna 29 och 30. Den rättsliga information som åsyftas är uppgifter om vilka krav som ställs på en framställning om rättslig hjälp och hur dessa krav skall kunna uppfyllas.

Hos Rikspolisstyrelsen finns sedan tidigare en operativ kontaktpunkt för bekämpning av högteknologisk brottslighet. Rikskriminalpolisens IT-brottsrotel har beredskap dygnet runt alla dagar i veckan, vilket innebär att det alltid går att nå en specialist på IT-brott. Utanför kontorstid går kontakten via Rikskommunikationscentralen. Kravet i artikel 35 på en kontaktpunkt som alltid är tillgänglig kan således uppfyllas.

Aktuella förslag till ändringar

Inom Europeiska unionen antog rådet för inrikes och rättsliga frågor den 29 maj 2000 en konvention om ömsesidig rättslig hjälp i brottmål (i fortsättningen kallad 2000 års EU-konvention). Ett tilläggsprotokoll antogs den 16 oktober 2001.

Inom Justitiedepartementet har utarbetats en promemoria med förslag om att Sverige skall tillträda konventionen och tilläggsprotokollet (Internationell rättslig hjälp i brottmål: Tillträde till 2000 års konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater m.m.; Ds 2004:50).

Promemorian innehåller förslag till de lagändringar som krävs för tillträde. Dessa lagförslag berör delvis samma frågor som behandlas i konventionen om IT-relaterad brottslighet. I promemorian föreslås att lagändringarna skall träda i kraft den 1 juli 2005.

Vad som är av särskilt intresse i detta sammanhang är att det i promemorian föreslås att rättslig hjälp skall ges med hemlig teleavlyssning och hemlig teleövervakning i betydligt större utsträckning än nu. Det föreslås att Sverige, förutom att för en annan stats räkning verkställa beslut om hemlig teleavlyssning eller hemlig teleövervakning, skall kunna ge en annan stat rättslig hjälp i form av tekniskt bistånd med hemlig teleavlyssning eller hemlig teleövervakning som verkställs av det landet. Vidare skall

rättslig hjälp även kunna omfatta gränsöverskridande hemlig teleavlyssning eller hemlig teleövervakning.

Utvidgningarna av det rättsliga samarbetet hänger bl.a. samman med förändringarna av tekniken på teleområdet, exempelvis satellittelefoni.

Om förslagen genomförs innebär det att rättslig hjälp med hemliga tvångsmedel på teleområdet kommer att ges i Sverige på tre olika sätt och med delvis olika beslutsregler. För det första kan svenska myndigheter under samma förutsättningar som i ett motsvarande svenskt fall besluta om och verkställa hemlig teleavlyssning eller hemlig teleövervakning i Sverige på begäran av en annan stat. För det andra kan en utländsk stat få tillåtelse att i Sverige själv verkställa ett i den staten meddelat beslut om hemlig teleavlyssning eller hemlig teleövervakning i form av gränsöverskridande tvångsmedel. För det tredje skall verkställighet av ett utländskt beslut om hemlig teleavlyssning eller hemlig teleövervakning kunna äga rum i Sverige genom att den utländska myndigheten får tekniskt bistånd med verkställigheten.

De föreslagna utvidgningarna av internationellt samarbete med hemliga tvångsmedel på teleområdet kommer även att kunna tillämpas av svenska åklagare, som kan ansöka om motsvarande hjälp i en annan stat.

Utvidgad användning av hemliga tvångsmedel på teleområdet ökar, som tidigare har nämnts, möjligheterna att utreda och lagföra IT-relaterad brottslighet där datakommunikation utgör en beståndsdel.

I den mån promemorian om tillträde till 2000 års EU-konvention innehåller förslag som har direkt betydelse för genomförandet av konventionen om IT-relaterad brottslighet redovisas de i det följande. De förslag i promemorian om tillträde till 2000 års EU-konvention som inte har betydelse för detta lagstiftningsärende men som berör paragrafer i vilka ändring föreslås som ett led i anpassningen till konventionen om IT-relaterad brottslighet beaktas inte här. Det får i stället bli en uppgift i det fortsatta lagstiftningsarbetet att samordna förslagen. En sådan samordning kan nämligen komma att kräva åtgärder som går utöver uppdra-

get att föreslå de lagändringar som krävs för en anpassning till konventionen om IT-relaterad brottslighet, exempelvis omarbetning eller omnumrering av paragrafer i vissa delar av lagen om internationell rättslig hjälp.

Promemorian har remissbehandlats och förslagen övervägs för närvarande inom regeringskansliet.

Behovet av åtgärder

Som framgått av redogörelsen för det svenska regelsystemet uppfyller lagen om internationell rättslig hjälp i allt väsentligt kraven i konventionen. Möjligheterna till rättslig hjälp kommer dessutom att öka om förslagen i promemorian om anpassning till 2000 års EU-konvention genomförs.

Om nya tvångsmedel eller andra utredningsbefogenheter tillskapas som ett led i anpassningen till konventionen om IT-relaterad brottslighet måste emellertid dessa få genomslag i det internationella samarbetet. Detta gäller särskilt de krav som ställs i artiklarna 29 och 30. Det krävs därför vissa lagstiftningsåtgärder för att följa upp sådana ändringar.

Bestämmelserna i artikel 27, som enbart är avsedda att användas i de fall där det inte finns någon lagstiftning eller någon överenskommelse mellan parterna (eller i de fall där parterna kommer överens om att tillämpa konventionens regler i stället), är väl förenliga med regelsystemet i lagen om internationell rättslig hjälp. Det finns dock inte någon regel om uppskjutande av verkställighet enligt artikel 27 punkt 5 i den svenska lagstiftningen, vilket kräver närmare överväganden.

6.13.2 Regler om utlämning m.m. (artikel 24)

Bedömning: De nuvarande reglerna om utlämning och överlämnande motsvarar kraven i konventionen.

Utlämningslagarna

Bestämmelser om utlämning för brott finns dels i lagen (1957:668) om utlämning för brott (utlämningslagen), dels i lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge (nordiska utlämningslagen).[33]

Enligt utlämningslagen får den som i en annan stat är misstänkt, tilltalad eller dömd för brott och som uppehåller sig här i landet utlämnas till den andra staten efter beslut av regeringen (1 §). Enligt huvudregeln skall den gärning för vilken utlämning begärs motsvara brott för vilket enligt svensk lag är föreskrivet fängelse i ett år eller mer (4 §). Är den som skall utlämnas svensk medborgare ställs högre krav på brottets svårhetsgrad (fängelse i mer än fyra år) och dessutom kan utlämning endast förekomma om det finns en särskild föreskrift om det (2 §). Svenska medborgare kan under vissa förutsättningar utlämnas till ett annat land inom den Europeiska unionen (3 §). För vissa brott (militära brott och politiska brott) får utlämning inte äga rum (5 § resp. 6 §). Vidare utlämnas inte den som på grund av sin härstamning, tillhörighet till en viss samhällsgrupp, religiösa eller politiska uppfattning eller annars på grund av politiska förhållanden riskerar allvarlig förföljelse i den främmande staten eller riskerar att lämnas vidare till en annan stat där han löper sådan risk (7 §). Utlämning kan vidare i vissa fall vägras av humanitära skäl. Beslut om utlämning fattas av regeringen, efter yttrande av riksåklagaren, som också skall verkställa utredning i utlämningsärendet (15 och 16 §§). Om den som begärs utlämnad inte samtycker till utlämningen skall ärendet dessutom prövas av Högsta domstolen, som avger ett yttrande (17 och 18 §§).

Inom den Europeiska unionen har tillämpats ett förenklat förfarande (28-40 §§). Vid samtycke till utlämning beslutar riksåklagaren om utlämning i uppenbara fall och i övrigt avgörs frå-

[33] Det finns regler om utlämning även i lagen (2002:329) om samarbete med Internationella brottmålsdomstolen och i lagen (1994:569) om Sveriges samarbete med de internationella tribunalerna för brott mot internationell humanitär rätt. Eftersom dessa lagar enbart är tillämpliga på ett fåtal brottstyper som saknar betydelse i detta sammanhang redovisas inte dessa regler här.

gan av regeringen. Dessa regler ersätts av den europeiska arresteringsordern (se nästa avsnitt).

I nordiska utlämningslagen ställs det inte lika stränga krav som för utlämning till andra länder. Den som i Danmark, Finland, Island eller Norge är misstänkt, tilltalad eller dömd för en där straffbelagd gärning och som uppehåller sig här i landet kan på begäran av den andra staten utlämnas dit (1 §). Det ställs inget särskilt krav på gärningen, utöver att utlämning inte får äga rum för en gärning som i den andra staten endast kan bestraffas med böter (3 §). En svensk medborgare utlämnas bara om han vid tiden för brottet sedan minst två år stadigvarande vistats i den stat som begär utlämning eller om utlämning begärs för brott för vilket enligt svensk lag är föreskrivet fängelse i mer än fyra år (2 §). Utlämning för politiskt brott kan bara ske om en gärning av motsvarande beskaffenhet är straffbelagd i Sverige (4 §). Svenska medborgare utlämnas inte för politiska brott. Förfarandet vid utlämning är förenklat. Om den som begärts utlämnad samtycker till utlämning beslutar åklagare, utom i de fall där det pågår en svensk förundersökning, åtal eller verkställighet av straff. I sådana fall, eller om den som begärs utlämnad inte samtycker till utlämning, beslutar normalt riksåklagaren om utlämning. I vissa fall skall beslutet fattas av regeringen (15 §).

Den europeiska arresteringsordern

En ny lag, som ersätter utlämningslagens bestämmelser om utlämning för brott till medlemsstater i EU, trädde i kraft den 1 januari 2004. Lagen bygger på det inom Europeiska unionen antagna rambeslutet om en europeisk arresteringsorder och om överlämnande mellan medlemsstaterna (prop. 2001/02:118, bet. 2001/02:JuU29 samt prop. 2003/04:7, bet. 2003/04:JuU8).

I förhållande till de nordiska länderna skall den nordiska utlämningslagen alltjämt gälla, i avvaktan på att den omarbetas. I fråga om utlämning till länder utanför Norden och EU gäller utlämningslagen även fortsättningsvis. Genom särskilda övergångsbestämmelser gäller alltjämt reglerna i utlämningslagen i

förhållande till EU-stater som inte har hunnit införliva rambeslutet.

Den nya lagstiftningen innebär i korthet följande. Lagen om överlämnande innehåller regler som delvis motsvarar bestämmelserna i utlämningslagarna. Den behandlar främst åklagares och domstolars handläggning och beslut i ärenden om överlämnande, som är den term som används i stället för utlämning. Lagen reglerar enbart överlämnanden från Sverige. I lagen anges när överlämnande skall beviljas. Reglerna motsvarar till stora delar vad som gäller för utlämning. För överlämnande för lagföring krävs det att gärningen enligt den begärande statens lagstiftning kan medföra fängelse i ett år eller mer. Enligt huvudregeln krävs det dubbel straffbarhet. Överlämnande kan dock i vissa fall beslutas även för gärningar som inte direkt motsvarar något brott enligt svensk lag. Sådana gärningar anges i en bilaga till lagen. Bland de uppräknade brotten kan nämnas barnpornografi, IT-brottslighet samt rasism och främlingsfientlighet.

Förfarandet vid överlämnande är enklare än vid utlämning. Beslut om överlämnande fattas av tingsrätt, vars beslut kan överklagas till hovrätten. Om prövningstillstånd beviljas kan frågan även prövas av Högsta domstolen. Tingsrätten skall i princip fatta beslut inom 30 dagar från det att den eftersökte greps. Om denne samtycker till överlämnande skall beslut fattas inom 10 dagar. Tvångsmedelsreglerna i den nya lagen avviker delvis från vad som gäller vid utlämning. Lagen föreskriver bl.a. en presumtion för att den som begärs överlämnad skall anhållas och häktas.

Ändringarna som föranletts av Sveriges antagande av rambeslutet står i samklang med de krav som konventionen om IT-relaterad brottslighet ställer.

Behovet av åtgärder

Bestämmelserna i artikel 24 i konventionen är avsedda att kunna tillämpas i de fall där det inte finns något utlämningsavtal eller någon annan motsvarande reglering eller i de fall där staterna kommer överens om att tillämpa konventionens regler i stället.

Reglerna i utlämningslagarna och i lagen om överlämnande från Sverige enligt en europeisk arresteringsorder står i god överensstämmelse med de krav som ställs i artikel 24. Det finns därför inget behov av lagstiftningsändringar.

6.13.3 Rambeslut om verkställighet av beslut om frysning av egendom eller bevismaterial

Riksdagen har nyligen godkänt ett inom Europeiska unionen upprättat utkast till rambeslut om verkställighet av beslut om frysning av egendom eller bevismaterial (prop. 2002/03:67, bet. 2002/03:JuU15). Rambeslutet innehåller bestämmelser som syftar till att dels säkerställa beslut om förverkande av egendom, dels säkerställa tillgång till bevismaterial i brottmål. Det samlande begreppet för dessa beslut är frysningsbeslut. Avsikten med rambeslutet är att genom enklare regler hindra att egendom som kan bli föremål för förverkande eller som behövs för bevisändamål går förlorad. Möjligheterna till frysning skall bl.a. kunna användas i det inledande skedet av en förundersökning då risken för att egendom försvinner eller förstörs ofta är störst.

Några förslag till lagstiftning lades inte fram i propositionen. Regeringen avser att återkomma till riksdagen med sådana förslag vid ett senare tillfälle.

Inom Justitiedepartementet har utarbetats en promemoria som innehåller förslag till en ny lag om erkännande och verkställighet inom Europeiska unionen av frysningsbeslut och till de övriga lagstiftningsändringar som krävs för att genomföra rambeslutet (Ju2004/11207/BIRS).

Begreppet frysning finns inte i svensk rätt. Ett frysningsbeslut motsvaras i den svenska lagstiftningen dels av reglerna i 26 kap. RB om kvarstad till säkrande av värdet av förverkad egendom, dels av reglerna om beslag i bevis- eller förverkandesyfte. I promemorian föreslås att en ny lag införs, som reglerar dels verkställighet i Sverige av utländska frysningsbeslut, dels hur svenska myndigheters motsvarande beslut skall utformas för att kunna verkställas i en annan EU-stat. Erkännande och verkställighet av

frysningsbeslut är enbart ett förstadium till ansökan om rättslig hjälp i brottmål eller om verkställighet av förverkandebeslut och skall regelmässigt följas av en ansökan om en sådan åtgärd. Den nya lagstiftningen föreslås träda i kraft den 1 juli 2005.

Promemorian är föremål för remissbehandling.

Den lagstiftning som krävs för att genomföra rambeslutet om frysning har marginell betydelse för anpassningen till konventionen om IT-relaterad brottslighet. Om förslagen genomförs underlättas dock tillämpningen av artikel 19 punkt 3 d.

6.14 Sekretess och uppgiftsskyldighet (del av artiklarna 20, 21 och 27)

6.14.1 Sekretessregler som berör konventionsåtagandena

Bedömning: De nuvarande reglerna i sekretesslagen uppfyller kraven i konventionen i fråga om befintliga tvångsmedel och i fråga om myndigheters televerksamhet. Däremot måste såväl frågan om sekretessreglerna är tillräckliga som frågan om eventuella begränsningar i meddelarfriheten övervägas om nya tvångsmedel införs.

Sekretessregler till skydd för brottsbekämpningen m.m.

En svensk framställning om rättslig hjälp omfattas av sekretessreglerna i 5 kap. 1 § sekretesslagen (sekretess till skydd för intresset att förebygga eller beivra brott) och 9 kap. 17 § sekretesslagen (sekretess till skydd för enskilds personliga och ekonomiska förhållanden).

I samband med att den nya lagen om internationell rättslig hjälp infördes tillkom även en sekretessbestämmelse till skydd för utländska framställningar om rättslig hjälp. Enligt 5 kap. 7 § sekretesslagen gäller sekretess i verksamhet som avser rättsligt samarbete på begäran av annan stat eller mellanfolklig domstol. Sekretessen gäller dels för utredning enligt bestämmelserna om

förundersökning, dels för angelägenhet som angår tvångsmedel, om det kan antas att det har varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas.

Med rättsligt samarbete[34] avses inte bara framställningar enligt lagen om rättslig hjälp utan även framställningar om utlämning (se prop. 1999/2000:61 s. 166). Med stöd av sekretessbestämmelsen kan bl.a. uppgifter om hemliga tvångsmedel på teleområdet (artikel 20 punkt 3 respektive artikel 21 punkt 3) hemlighållas. Detsamma gäller själva ansökan om hjälp (artikel 27 punkt 8). Regeln är generellt utformad och täcker därigenom även ny lagstiftning om rättsligt samarbete.

En domstol som håller förhandling i en fråga som rör internationell rättslig hjälp kan enligt 5 kap. 1 § andra stycket RB hålla förhandling inom stängda dörrar om det vid förhandlingen avhandlas frågor som skyddas av sekretess enligt 5 kap. 1 eller 7 § eller 9 kap. 17 § sekretesslagen.

Det råder meddelarfrihet för de flesta av de uppgifter som omfattas av sekretess enligt nu angivna bestämmelser. I fråga om hemliga tvångsmedel gäller dock inte meddelarfrihet (16 kap. 1 § sekretesslagen).

Vid begäran om rättslig hjälp från en annan stat gäller sekretess enligt 9 kap. 17 § sekretesslagen till skydd för enskild.

Sekretessregler till skydd för myndigheters televerksamhet

För myndigheter som bedriver televerksamhet tillämpas 9 kap. 8 § och 14 kap. 2 § sekretesslagen i stället för reglerna om tystnadsplikt i lagen om elektronisk kommunikation. Bestämmelserna i 9 kap. 8 § sekretesslagen motsvarar i huvudsak regleringen i 6 kap. 20 § lagen om elektronisk kommunikation. Den sekretessbrytande bestämmelsen i 14 kap. 2 § sekretesslagen är dock delvis annorlunda utformad. Uppgift som angår misstanke om brott får enligt huvudregeln i denna paragraf lämnas till åkla-

[34] Tidigare användes termen ”rättslig hjälp” i sekretessbestämmelsen. Den ersattes nyligen med termen rättsligt samarbete.

garmyndighet, polismyndighet eller annan myndighet som har att ingripa mot brottet, om fängelse är föreskrivet för brottet och detta kan antas ge annan påföljd än böter. Uppgifter som omfattas av sekretess enligt 9 kap. 8 § (t.ex. uppgifter som rör ett telemeddelande eller innehållet i detta) kan dock enbart lämnas vid misstanke om brott som bestraffas med lägst två års fängelse. Regleringen avseende uppgifter om abonnemang överensstämmer med vad som gäller enligt lagen om elektronisk kommunikation.

Uppgifter kan lämnas ut antingen på begäran (jfr 15 kap. 5 § sekretesslagen) eller på myndighetens eget initiativ. Det är den utlämnande myndigheten som bedömer om kraven för utlämnande är uppfyllda.

Det är osäkert om de nu redovisade sekretessreglerna har någon praktisk betydelse, men de uppfyller de krav som anges i artiklarna 20 punkt 3 och 21 punkt 3.

Förslag till ändringar

Sekretesslagen har nyligen setts över av Offentlighets- och sekretesskommittén. Kommittén har bl.a. föreslagit en helt ny sekretesslag (SOU 2003:99). Betänkandet har remissbehandlats.

Förslaget till ny sekretesslag innebär i sak inga förändringar som har betydelse för detta lagstiftningsärende.

Behovet av åtgärder

De nuvarande sekretessbestämmelserna uppfyller kraven i konventionen. Om nya tvångsmedel införs måste emellertid såväl frågan om de nuvarande sekretessreglerna är tillräckliga som behovet av eventuella begränsningar i meddelarfriheten övervägas.

6.14.2 Tystnadsplikt för teleoperatörer m.fl.

Bedömning: De nuvarande reglerna om tystnadsplikt för operatörer m.fl. uppfyller kraven i konventionen. Om nya tvångsmedel införs måste dock frågan om tystnadspliktens omfattning tas under förnyat övervägande.

Regler om tystnadsplikt för teleoperatörer på den allmänna marknaden och för den som tillhandahåller elektroniska kommunikationsnät eller elektroniska kommunikationstjänster finns i lagen om elektronisk kommunikation.

Enligt 6 kap. 20 § lagen om elektronisk kommunikation får den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till

1. uppgift om ett abonnemang,
2. innehållet i ett elektroniskt meddelande eller
3. annan uppgift som angår ett särskilt elektroniskt meddelande

inte obehörigen föra vidare eller utnyttja det han fått del av eller tillgång till.

Tystnadsplikten gäller inte i förhållande till dem som deltagit i utväxlingen av meddelandet eller som på annat sätt har sänt eller tagit emot ett sådant meddelande. Tystnadsplikten enligt punkterna 1 och 3 gäller inte heller i förhållande till innehavaren av ett abonnemang som använts för ett elektroniskt meddelande.

Enligt 6 kap. 21 § har operatörer dessutom tystnadsplikt beträffande användning av vissa hemliga tvångsmedel, nämligen hemlig teleavlyssning, hemlig teleövervakning och kvarhållande av försändelse. Denna tystnadsplikt gäller även mot abonnenten.

Reglerna om tystnadsplikt uppfyller de krav som ställs i artiklarna 20 punkt 3 och 21 punkt 3 beträffande befintliga tvångsmedel. Om det införs nya tvångsmedel måste frågan om tystnadspliktens omfattning övervägas i det sammanhanget.

6.15 Informationsutbyte m.m. (artiklarna 26 och 28)

6.15.1 Informationsutbyte

Bedömning: Någon ändring i lagstiftningen som reglerar informationsutbyte behövs inte för anpassningen till konventionen.

Sekretesslagen innehåller inga generella regler om informationsutbyte. Sådana uppgifter som inte är föremål för sekretess kan alltid utbytas, om det inte finns någon annan bestämmelse som lägger hinder i vägen. I vad mån det är tillåtet att lämna sekretessbelagd information får avgöras från fall till fall. Det kan emellertid finnas anledning att erinra om att bestämmelserna om sekretess inte bara gäller till skydd för svenska fysiska eller juridiska personer utan skyddar också utländska medborgare och företag (Göran Regner m.fl. Kommentar till sekretesslagen s. I:12).

Den grundläggande bestämmelsen om utlämnande av sekretessbelagda uppgifter till utländsk myndighet finns i 1 kap. 3 § tredje stycket sekretesslagen. Enligt huvudregeln får uppgift för vilken sekretess gäller inte röjas för en utländsk myndighet annat än om utlämnandet sker enligt särskild föreskrift i lag eller förordning. Bestämmelsen medför ingen förpliktelse att lämna ut uppgifter utan reglerar enbart under vilka förutsättningar det är tillåtet att lämna uppgifter till en utländsk myndighet eller internationell organisation. Regler om utlämnande finns bl.a. i olika lagar om internationellt samarbete i fråga om verkställighet.

En sekretessbelagd uppgift får även lämnas ut om uppgiften i motsvarande fall skulle få lämnas ut till svensk myndighet och det enligt den utlämnande myndighetens prövning står klart, att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten. Prövningen av om uppgiftslämnandet är förenligt med svenska intressen skall göras av myndigheten som sådan. Det innebär att en enskild tjänsteman inte får besluta i en sådan fråga annat än om han enligt arbetsordningen,

tjänsteföreskrifter eller annat beslut har fått behörighet att besluta på myndighetens vägnar (a.a. s. 1:13).

Bestämmelsen om spontant uppgiftslämnande i artikel 26 innebär inget åtagande att lämna information. Härigenom lämnas det åt staterna att avgöra i vilken utsträckning den inhemska lagstiftningen medger informationsutbyte över gränserna. Någon anpassning till konventionen är således inte nödvändig. Det finns inte heller något skäl att ändra det nuvarande regelsystemet, som bygger på en noggrann avvägning mellan olika motstående intressen.

6.15.2 Villkor om användningsbegränsning

Bedömning: Det behövs inga lagändringar för att uppfylla kraven på bestämmelser om användningsbegränsning i konventionen.

Nuvarande bestämmelser

Har en svensk myndighet i ett ärende om rättslig hjälp fått uppgifter eller bevisning från en annan stat enligt en internationell överenskommelse, som är bindande för Sverige och som innehåller villkor som begränsar möjligheterna att använda uppgifterna eller bevisningen vid utredning av brott eller i ett rättsligt förfarande med anledning av brott, skall, enligt 5 kap. 1 § lagen om internationell rättslig hjälp, svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning. Bestämmelsen har i sak oförändrad förts över från lagen (1991:435) med vissa bestämmelser om internationellt samarbete på brottmålsområdet. Likartade bestämmelser om användningsbegränsning finns i lagen (2000:343) om internationellt polisiärt samarbete, lagen (2000:344) om Schengens informationssystem samt lagen (2000:1219) om internationellt tullsamarbete.

Bestämmelserna om användningsbegränsning innebär bl.a. att skyldigheten att inleda förundersökning och åtalsplikten får vika för det överenskomna villkoret (prop. 1990/91:131 s. 23).

De nuvarande reglerna om användningsbegränsning uppfyller kraven i artikel 28 punkt 2 b. Däremot torde den nuvarande regleringen inte täcka uppgifter som lämnas spontant med stöd av artikel 26, som också förutsätter att den som lämnar uppgifterna skall kunna ställa krav på hur de används.

Förslag till ändringar

I den tidigare nämnda promemorian om tillträde till 2000 års EU-konvention (se avsnitt 6.13.1) har föreslagits (s. 212) att regeln i 5 kap. 1 § lagen om internationell rättslig hjälp förtydligas och utvidgas till att omfatta även uppgifter om bevisning som lämnas utan samband med ett ärende om rättslig hjälp. Om ändringen genomförs får den betydelse för tillämpningen av artikel 26 i konventionen på det sättet att svenska myndigheter får möjlighet att tillgodose en utländsk myndighets krav på användningsbegränsning när uppgifter lämnas spontant. En motsvarande ändring har föreslagits i 5 kap. 2 §, som reglerar de villkor som en svensk myndighet kan ställa när den ger rättslig hjälp.

Behovet av åtgärder

Om de nyss nämnda förslagen till ändringar i lagen om internationell rättslig hjälp genomförs behövs det inte någon ytterligare lagändring för att uppfylla kraven i konventionen.

6.16 Övriga bestämmelser (artiklarna 1-2 och 36-48)

Bedömning: Övriga delar av konventionen kräver inte någon anpassning av den svenska lagstiftningen. Frågan om Sverige bör göra förbehåll i förhållande till någon artikel eller använda

möjligheten att ställa upp särskilda rekvisit behandlas närmare i övervägandena.

Artiklarna 1 och 2 innehåller inga krav på anpassning av den nationella rätten.

Frågan om Sverige bör göra förbehåll i något avseende (artikel 42) eller utnyttja möjligheten att uppställa särskilda rekvisit (artikel 40) tas upp under övervägandena i det följande (avsnitt 11.11). I övrigt innehåller artiklarna 36–48 inte något som kräver lagstiftningsåtgärder.

6.17 Sammanfattning av lagstiftningsbehovet vid tillträde till konventionen

Bedömning: Svensk rätt uppfyller i stor utsträckning de krav som konventionen ställer. Det krävs emellertid lagstiftning för att helt uppfylla kraven i vissa artiklar

I tidigare avsnitt har redovisats på vilka punkter den svenska lagstiftningen för närvarande inte uppfyller de krav som konventionen ställer. I de allra flesta avseenden är kraven redan uppfyllda, men det krävs anpassning för att Sverige skall leva upp till kraven i vissa artiklar.

På det straffrättsliga området krävs det få ändringar. Vissa ändringar i reglerna i 4 kap. BrB är nödvändiga för att kraven i artiklarna 3, 4 och 5 skall uppfyllas helt. Vidare krävs det lagstiftningsåtgärder för att kraven i artikel 7 på kriminalisering av dataförfalskning skall uppfyllas.

Inom det straffprocessuella området krävs det fler ändringar. Utöver reglerna om hemliga tvångsmedel på teleområdet, och det i brottmål mindre användbara institutet edition, finns det inte några bestämmelser som svarar upp till kraven i artikel 16 på att enskilda skall kunna åläggas att temporärt bevara lagrad information. Den nuvarande lagstiftningen ger inte heller utrymme för att, i enlighet med artikel 19 punkt 4, ålägga någon att lämna

information om ett visst datorsystem i syfte att underlätta verkställighet av tvångsmedel. Reglerna om beslag och husrannsakan måste också anpassas för att fungera bättre i IT-miljö. Den svenska lagstiftningen uppfyller inte heller i alla delar kraven i artiklarna 20 och 21, som avser hemlig teleavlyssning och hemlig teleövervakning. För att möjliggöra snabb tillgång till trafikuppgifter i enlighet med artikel 17 krävs det också lagändringar.

Lagstiftningen om internationellt samarbete uppfyller i allt väsentligt de krav som ställs i konventionen. För att anpassningarna av den straffprocessuella lagstiftningen skall få genomslag i det internationella samarbetet krävs det emellertid att de nya tvångsmedlen och utredningsbefogenheterna får motsvarighet i uppräkningen i lagen om internationell rättslig hjälp av åtgärder med vilka Sverige ger andra stater bistånd. De ändringar som krävs är framför allt hänförliga till artiklarna 29 och 30. Det krävs även överväganden beträffande krav i artikel 27 punkt 5.

De nuvarande sekretessreglerna och reglerna om tystnadsplikt uppfyller kraven i konventionen, men om det införs nya tvångsmedel och utredningsbefogenheter måste såväl frågan om reglerna är tillräckliga som frågan om eventuella begränsningar i meddelarfriheten tas under övervägande.

7 Tilläggsprotokollets överensstämmelse med svensk rätt

7.1 Allmänt om tilläggsprotokollet

Tilläggsprotokollet behandlar frågan om kriminalisering av gärningar av rasistisk eller främlingsfientlig natur. Protokollet omfattar enbart sådana gärningar som begås med hjälp av datorsystem. Begås brotten på annat sätt faller de utanför tillämpningsområdet.

Den snabba utvecklingen av framför allt Internet har både för- och nackdelar från informations- och yttrandefrihetssynpunkt. Å ena sidan kan vem som helst snabbt, enkelt och billigt distribuera stora mängder information. Den stora informationsmängden och lättillgängligheten leder också till att betydligt fler kan få del av samma information samtidigt. Möjligheten att lägga ut information på Internet innebär vidare att även den som har udda, obekväma eller rentav förargelseväckande åsikter, som normalt inte sprids av etermedier eller trycks av förlag, har möjlighet att förmedla dessa till en större krets. Å andra sidan innebär den ökade tillgängligheten att även material som exempelvis barnpornografi och främlingsfientliga alster, som inte borde spridas därför att det i sig är kriminaliserat eller därför att det uppmuntrar till brott, snabbt kan spridas över ett stort område och till en stor mängd personer. Spridningen får härigenom betydligt större genomslagskraft än när material av motsvarande slag framställs och sprids med traditionell teknik. Upphovsmannen eller spridaren kan också utnyttja sig av den anonymitet som Internet erbjuder för att dölja sin identitet. Tilläggsprotokollet

aktualiserar därför frågor angående informations-, yttrande- och tryckfrihet.

Såväl som TF som YGL innehåller regler som straffbelägger gärningar av rasistisk och främlingsfientlig natur. Motsvarande allmänna brott finns i brottsbalken. TF och YGL innehåller också processuella bestämmelser som i vissa delar avviker från rättegångsbalkens reglering. I det följande redovisas regelsystemen var för sig under olika rubriker.

7.2 Yttrandefriheten och tilläggsprotokollet

7.2.1 Kort om det yttrandefrihetsrättsliga systemet

Enligt 2 kap. 1 § regeringsformen (RF) tillförsäkras varje medborgare yttrande- och informationsfrihet. Med yttrandefrihet åsyftas friheten att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt att uttrycka tankar, åsikter och känslor. Med informationsfrihet åsyftas friheten att hämta in och ta emot upplysningar samt att i övrigt ta del av andras yttranden. Dessa friheter får inskränkas genom lag. Sådana begränsningar får emellertid inte göras för vilka ändamål eller i vilken omfattning som helst. I 2 kap. 12 § RF föreskrivs att begränsning i nu nämnda friheter, samt vissa andra friheter som bl.a. mötes-, demonstrations- och religionsfriheten, får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En sådan begränsning får dessutom aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Begränsning får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Enligt 2 kap. 13 § RF gäller dessutom särskilda restriktioner för begränsningar av yttrandefriheten och informationsfriheten. Dessa friheter får enbart begränsas med hänsyn till rikets säkerhet, folkförsörjningen, allmän ordning och säkerhet, enskilds anseende, privatlivets helgd eller förebyggandet och beivrandet av brott. Friheten att yttra sig i näringsverksamhet får också be-

gränsas. I övrigt får begränsningar av yttrandefriheten och informationsfriheten ske endast om särskilt viktiga skäl föranleder det.

Sedan den 1 januari 1995 gäller Europakonventionen som svensk lag. I artikel 10 i konventionen ges regler till skydd för yttrandefriheten som i allt väsentligt motsvarar reglerna i RF.

Friheten att yttra sig i tryckt skrift skyddas särskilt i TF. Ett motsvarande skydd för friheten att yttra sig genom ljudradio, television och vissa liknande överföringar samt i filmer, videogram, ljudupptagningar och andra tekniska upptagningar finns i YGL. Dessa lagar bygger på några grundläggande principer av vilka de i detta sammanhang viktigaste är

- förbud mot censur och hindrande åtgärder,
- ensamansvar med meddelarskydd,
- särskild brottskatalog och
- särskild rättegångsordning.

Förbudet mot censur innebär att framställning och spridning av tryckta skrifter samt motsvarande åtgärder beträffande medier som regleras i YGL inte får villkoras av förhandsgranskning av det allmänna. Censurförbudet i TF är absolut, medan censurförbudet i YGL har försetts med undantag. För en närmare redovisning hänvisas till SOU 2001:28 s. 94.

Förbudet mot hindrande åtgärder innebär att det allmänna inte får, på grund av innehållet i en tryckt skrift eller ett medium som avses i YGL, hindra framställning och spridning (eller motsvarande åtgärder i fråga om medium som regleras i YGL) på annat sätt än som är medgivet i TF resp. YGL.

En av de grundläggande principerna i TF och YGL är principen om ensamansvar. Den innebär att endast en av de personer som har deltagit i tillkomsten av en grundlagsskyddad framställning bär det straffrättsliga ansvaret för innehållet i denna och att det i grundlagarna anges vem denna person är. Övriga medverkande går fria från ansvar. TF och YGL innehåller vidare en ansvarskedja, som anger vem ansvaret faller på om inte personen närmast före i kedjan kan åläggas ansvar. Det straffrättsliga ansvaret är således dels exklusivt, dels successivt. Det är också for-

mellt i den meningen att det faller på den i TF resp. YGL utpekade personen oavsett hur han har bidragit till framställningen eller vad han har känt till om innehållet i denna.

Vissa typer av yttranden anses utgöra så allvarligt missbruk av tryck- och yttrandefriheten att de straffbeläggs som tryck- respektive yttrandefrihetsbrott. Dessa brott anges i en uttömmande uppräkning i 7 kap. 4 § TF, till vilken bestämmelse 5 kap. 1 § YGL hänvisar. Ingripanden mot sådana brott får bara förekomma i de fall och den utsträckning som anges i TF och YGL. För att ett tryckfrihets- eller ett yttrandefrihetsbrott skall kunna leda till straffansvar krävs det att gärningen är straffbar enligt lag. Det krävs alltså dubbel straffbarhet. I fråga om påföljderna för tryckfrihets- och yttrandefrihetsbrott hänvisar TF resp. YGL till brottsbalken.

Reglerna om åtal och rättegång är i huvudsak desamma i TF och YGL (9 och 12 kap. TF resp. 7 och 9 kap. YGL). Justitiekanslern är ensam åklagare i mål av detta slag. Frågan om det föreligger brott prövas av en jury om nio personer, om inte parterna avstår från det. Juryns utslag anses fällande om minst sex jurymedlemmar har röstat för att brott har begåtts. Vid fällande juryutslag skall målet prövas av rätten, som antingen kan fria eller fälla. Har juryn meddelat friande utslag är detta däremot bindande för rätten.

Både TF och YGL gäller främst för sådant som produceras och sprids i Sverige. I viss utsträckning är reglerna även tillämpliga på utländska yttranden. För en närmare redogörelse se SOU 2001:28 s. 101 f.

Grundlagsskyddet har gjorts mera teknikoberoende genom ändringar i prop. 2001/02:74. Ändringarna, som bygger vidare på det befintliga systemet för tryck- och yttrandefrihet, har främst intresse för utvecklingen av nya tjänster på Internet. Grundlagsskyddet för vissa typer av framställningar och databaser har utökats.

7.2.2 Regleringen i tilläggsprotokollet

Som tidigare har nämnts (avsnitt 5.2.2) innehåller ingressen till tilläggsprotokollet en text som gör klart att protokollet inte är avsett att påverka etablerade principer i nationell rätt som rör yttrandefrihet. Texten tillkom på svenskt initiativ, mot bakgrund av de särregler för tryck- och yttrandefrihet som gäller i svensk rätt. Initiativet stöddes emellertid av flera andra länder, varför undantaget kom att få en generell utformning.

För svensk del innebär undantaget i ingressen att de principer på yttrandefrihetens område som är reglerade i grundlag inte påverkas av protokollet. Några grundlagsändringar behövs därför inte. En av artiklarna, artikel 3 punkt 3, innehåller dessutom i sig en hänvisning till sådana principer i nationell rätt.

Undantaget omfattar givetvis även andra principer är enbart de som rör tryckfrihets- och yttrandefrihetsbrott, t.ex. informationsfriheten enligt RF.

7.3 Straffrättsliga frågor

7.3.1 Allmänna utgångspunkter

I artikel 2 i tilläggsprotokollet finns det en definition av vad som avses med rasistiskt och främlingsfientligt material. Med detta avses skrivet material, bild eller annan framställning av idéer eller teorier som förespråkar, främjar eller uppmanar till hat, diskriminering eller våld mot en enskild person eller en grupp av personer på grund av ras, hudfärg, härstamning eller nationellt eller etniskt ursprung samt trosbekännelse, om något av dessa karakteristika åberopas. Det finns inte något formellt krav på att definitionen skall införas i den nationella rätten, men det förutsätts att det i så fall finns motsvarande bestämmelser.

Definitionen i artikel 2, som knyter an till vad som skall kriminaliseras enligt artikel 3, stämmer väl överens med hur det straffbara området har avgränsats i bestämmelsen om hets mot folkgrupp (se nedan). Det finns dock ett undantag. Begreppet

härstamning (descent), som används i tilläggsprotokollet, finns varken bland rekvisiten i bestämmelsen om hets mot folkgrupp eller i andra straffbestämmelser som innehåller liknande rekvisit. I svensk rätt motsvarar emellertid uttrycket nationellt och etniskt ursprung vad som åsyftas med härstamning i tilläggsprotokollet (se den förklarande rapporten punkt 18, av vilken det framgår att det inte är socialt ursprung som åsyftas).

I likhet med vad som är fallet med de gärningar som behandlas i konventionen tar tilläggsprotokollet enbart sikte på uppsåtligt handlande. Vidare används termen ”without right” på samma sätt som i konventionen (se avsnitt 4.3.1) för att avgränsa det straffbara området.

7.3.2 Spridande av rasistiskt och främlingsfientligt material (artikel 3)

Bedömning: Det behövs inga lagstiftningsåtgärder för att uppfylla åtagandena i artikel 3. Regleringen av tryck- och yttrandefrihetsbrott innebär dock vissa begräsningar som medför att möjligheten att avge förbehåll bör övervägas.

Enligt artikel 3 skall varje part vidta nödvändiga åtgärder för att straffbelägga att någon till allmänheten med hjälp av datorsystem sprider eller på annat sätt gör tillgängligt rasistiskt och främlingsfientligt material.

En part får förbehålla sig rätten att inte införa straffansvar när materialet förespråkar, främjar eller uppmuntrar diskriminering utan samband med hat eller våld. En förutsättning för detta är att det finns andra effektiva åtgärder. Vidare får en part förbehålla sig rätten att inte tillämpa kravet på straffansvar vid de fall av diskriminering för vilka parten inte kan föreskriva åtgärder på grund av etablerade principer om yttrandefrihet.

Allmänna brott

Nuvarande bestämmelser

Den som i ett uttalande eller i annat meddelande som sprids hotar eller uttrycker missaktning för en folkgrupp eller annan sådan grupp av personer med anspelning på bl.a. ras, hudfärg, nationellt eller etniskt ursprung eller trosbekännelse, döms enligt 16 kap. 8 § BrB för hets mot folkgrupp. Bestämmelsen arbetades om i samband med att Sverige ratificerade FN:s konvention om avskaffande av alla former av rasdiskriminering, i syfte att anpassa den till den konventionens krav på kriminalisering.

Utanför det straffbara området för hets mot folkgrupp faller omdömen som inte överskrider gränsen för en saklig kritik av vissa raser eller folkgrupper. Under lagstiftningsarbetet påpekades att det kan uppstå tillämpningsproblem när man skall avgöra var gränsen går mellan sakligt befogad kritik, som är tillåten, och straffbar missaktning. Första lagutskottet framhöll att begreppet missaktning måste tolkas med viss försiktighet.

Bestämmelsen skyddar kollektivt bestämda grupper. Enstaka identifierbara individer omfattas däremot inte av skyddet. Det innebär bl.a. att en målsägande inte kan föra talan om hets mot folkgrupp (NJA 1978 s. 3).

Straffregeln ställer inget krav på att hotet eller uttrycket för missaktning direkt avser gruppens ras, hudfärg eller motsvarande kriterium. Inte bara direkta utan även indirekta uttryck för missaktning faller därför inom det straffbara området (NJA 1982 s. 128).

Ett uttalande behöver inte göras offentligen för att vara straffbart som hets mot folkgrupp. Det är tillräckligt att uttalandet eller meddelandet sprids. Med spridning avses att uttalandet eller meddelandet når en grupp människor som utgör mer än ett fåtal (se bl.a. NJA 1999 s. 702). I uttrycket sprida uttalande ligger såväl att själv göra ett uttalande som att sprida vad man har hört av någon annan. Spridandet kan också bestå i att någon på allmän plats öppet bär symboler som anses starkt förknippade med åsikter av rasistisk innebörd (NJA 1996 s. 577).

Som tidigare nämnts (avsnitt 5.2.3) omfattar begreppet ”göra tillgängligt” skapande och kompilering av hyperlänkar. I fråga om åtgärder av detta slag torde frågan om gärningsmannens uppsåt ofta bli avgörande.

Straffet för hets mot folkgrupp är fängelse i högst två år eller, om brottet är ringa, böter.

Genom en lagändring som trädde i kraft den 1 januari 2003 har en särskild straffskala för grova brott införts. Den tillkom för att motverka de rasistiska sammanslutningar som växt fram och deras ökande propagandaverksamhet. Är brottet grovt är straffet fängelse i lägst sex månader och högst fyra år. Vid bedömningen av om brottet är grovt skall särskilt beaktas om meddelandet haft ett särskilt hotfullt eller kränkande innehåll och spritts till ett stort antal personer på ett sätt som varit ägnat att väcka betydande uppmärksamhet. Det krävs således både att uttalandet klart har överskridit gränsen för det tillåtna och att meddelandet har spritts i stor omfattning för att en gärning skall bedömas som grov (prop. 2001/02:59 s. 27). Uttalanden som gjorts tillgängliga på Internet torde som regel väl uppfylla det sistnämnda kravet. Detsamma torde gälla meddelanden på en elektronisk anslagstavla. Om uttalandena också uppfyller det förstnämnda kriteriet får avgöras i det enskilda fallet.

I samband med att straffansvaret för hets mot folkgrupp skärptes gjorde regeringen vissa uttalanden angående straffvärdet för hets mot folkgrupp. Det framhölls att om någon i stor skala och till en vid krets sprider alster med rasistiskt och liknande innehåll, kan detta ur straffvärdesynpunkt inte jämställas med att någon i en trängre krets vid enstaka tillfälle uttalar sig kränkande på ett sätt som utgör hets mot folkgrupp (a. prop. s. 26).

Hets mot folkgrupp är inte kriminaliserat på försöks-, förberedelse- eller stämplingsstadiet. Detta skall ses mot bakgrund av att sådana brott ofta begås i framställningar som omfattas av regleringen i TF och YGL, där censurförbudet och förbudet mot hindrande åtgärder lägger hinder i vägen mot kriminalisering innan brottet har fullbordats och att det även utanför TF:s och YGL:s tillämpningsområde skulle vara svårt att åstadkomma en

sådan reglering utan att komma i konflikt med grundlagsskyddade fri- och rättigheter.

Ett annat brott som bör nämnas i sammanhanget är *uppvigling*. För uppvigling döms enligt 16 kap. 5 § BrB bl.a. den som i skrift som sprids eller lämnas ut för spridning eller i annat meddelande till allmänheten uppmanar till eller försöker förleda till brottslig gärning (exempelvis hets mot folkgrupp). Försök och förberedelse till uppvigling är inte straffbart, vilket skall ses mot bakgrund av brottets konstruktion.

Straffet för uppvigling är böter eller fängelse i högst sex månader. Om brottet är att anse som grovt, med hänsyn till att gärningsmannen har sökt förleda till allvarligt brott eller av annat skäl, är straffet fängelse i högst fyra år. I ringa fall av uppvigling skall inte dömas till ansvar. Vid bedömningen av om det är fråga om ett ringa fall skall särskilt beaktas om det har förelegat endast obetydlig fara för att uppmaningen eller försöket skulle leda till efterföljd.

I lagen om elektroniska anslagstavlor finns det också regler som syftar till att förhindra spridning av rasistiska och främlingsfientliga uttalanden. Den som tillhandahåller en elektronisk anslagstavla är, som tidigare nämnts (avsnitt 6.5.1), skyldig att hålla uppsikt över innehållet på anslagstavlan (4 §). I uppgiften ingår att ta bort eller på annat sätt förhindra spridning av vissa meddelanden med brottsligt innehåll (5 § första stycket 1). I en särskild uppräkning anges vilka typer av meddelanden som skall tas bort. Till sådana hör meddelanden vilkas innehåll uppenbart är sådant som avses i bestämmelserna om uppvigling och hets mot folkgrupp. Den som uppsåtligen eller av grov oaktsamhet bryter mot denna skyldighet döms till böter eller fängelse i högst sex månader (7 §). Om brottet är grovt är straffet fängelse i högst två år. I ringa fall skall inte dömas till ansvar. Straffbestämmelsen är subsidiär till reglerna i brottsbalken (7 § andra stycket).

För olaga diskriminering (16 kap. 9 § BrB) döms en näringsidkare som i sin verksamhet tillämpar andra villkor mot någon på grund av hans ras, hudfärg, nationella eller etniska ursprung eller

trosbekännelse. Straffet är böter eller fängelse i högst ett år. Bestämmelsen har ett helt annat tillämpningsområde än artikel 3 och övriga artiklar i tilläggsprotokollet och saknar därför betydelse i detta sammanhang.

Bedömning

Bestämmelserna om hets mot folkgrupp och uppvigling uppfyller kraven i artikel 3. Det behövs därför inga lagändringar.

Tryck- och yttrandefrihetsbrott

Hets mot folkgrupp varigenom någon hotar eller uttrycker missaktning för folkgrupp eller annan sådan grupp av personer med anspelning på ras, hudfärg, nationellt eller etniskt ursprung, trosbekännelse eller sexuell läggning tillhör de brott som räknas upp i brottskatalogen i 7 kap. 4 § TF (p. 11). Detsamma gäller uppvigling (p. 10). Sådant handlande kan, genom hänvisningen i 5 kap. 1 § YGL till nyss nämnda bestämmelse, även bestraffas som yttrandefrihetsbrott.

Regleringen i TF och YGL innebär att det finns möjlighet att ingripa mot gärningar av det slag som behandlas i artikel 3 även i de fall där brottet begås i ett grundlagsskyddat medium. Den särskilda regleringen innebär emellertid begränsningar t.ex. i fråga om vem som kan göras ansvarig för brottet. Möjligheten att avge förklaring enligt artikel 3 punkt 3 att straffansvar inte införs i de fall ett sådant ansvar skulle strida mot den svenska regleringen av yttrandefriheten måste därför övervägas. Frågan om förbehåll behandlas vidare i avsnitt 11.11.

7.3.3 Rasistiskt eller främlingsfientligt motiverat hot eller kränkning (artiklarna 4 och 5)

Bedömning: Det krävs inga lagstiftningsåtgärder för att uppfylla kraven i artiklarna 4 och 5. Möjligheten att göra förbehåll enligt artikel 5 bör dock övervägas, mot bakgrund av den särskilda regleringen av tryck- och yttrandefrihetsbrott.

Det som enligt artikel 4 skall vara kriminaliserat är följande: att med hjälp av ett datorsystem antingen hota en person, av det skälet att personen tillhör en grupp som utmärks av ras, hudfärg, härstamning, trosbekännelse eller etniskt eller nationellt ursprung, under förebärande av något av nämnda karakteristiska, eller en grupp av personer som kännetecknas på nyss angivet sätt, med att begå ett allvarligt brott.

Det finns inget utrymme för att göra förbehåll eller på annat sätt inskränka tillämpningen av artikel 4.

Enligt artikel 5 skall det vara straffbart att med hjälp av ett datorsystem offentligen kränka en person, av det skälet att personen tillhör en grupp som utmärks av ras, hudfärg, härstamning, trosbekännelse eller etniskt eller nationellt ursprung, under förebärande av något av nämnda karakteristiska, eller en grupp av personer som kännetecknas på nyss angivet sätt.

En part får ställa krav på att brott som avses i artikel 5 resulterar i att personen eller gruppen av personer utsätts för hat, missaktning eller löje. En part har även möjlighet att förbehålla sig rätten att, helt eller delvis, inte tillämpa artikeln.

Allmänna brott

Nuvarande bestämmelser

Att hota någon med brottslig gärning på sätt som är ägnat att hos den hotade framkalla allvarlig fruktan för egen eller annans säkerhet till person eller egendom är enligt 4 kap. 5 § BrB straffbelagt som *olaga hot*. Hotet behöver inte uttryckas offentligt.

Motiven för hotet saknar betydelse för straffansvaret. Däremot kan ett rasistiskt motiv ha betydelse för påföljdsvalet och straffmätningen.

Straffet för olaga hot är böter eller fängelse i högst ett år. Är brottet grovt är straffet fängelse lägst sex månader och högst fyra år.

Den som i ett uttalande eller i annat meddelande som sprids hotar eller uttrycker missaktning för folkgrupp eller annan sådan grupp av personer med anspelning på ras, hudfärg, nationellt eller etniskt ursprung eller trosbekännelse gör sig, som nyss har redovisats, skyldig till *hets mot folkgrupp*.

Uttrycket hotar i bestämmelsen om hets mot folkgrupp skall tolkas enligt vanligt språkbruk och omfattar således inte bara sådant handlande som har kriminaliserats som olaga hot eller olaga tvång (Holmqvist m.fl. s. 16:36).

Med uttrycket missaktning avses att även andra kränkande omdömen än sådana som kan bedömas som förtal eller smädelser som kan vara straffbara som hets mot folkgrupp. Även företeelser som innebär att en viss ras eller folkgrupp förlöjligas torde praktiskt taget alltid falla in under bestämmelsen (Holmqvist m.fl. s. 16:36).

Som framgått ovan täcker bestämmelsen om hets mot folkgrupp även kränkningar och hot som riktar sig mot enstaka företrädare för den utpekade folkgruppen eller motsvarande, men det får inte vara fråga om identifierbara individer.

Även ansvar för *uppvigling* kan aktualiseras, t.ex. att någon uppviglar andra till hets mot folkgrupp.

Bestämmelser om ärekränkning finns i 5 kap. BrB. Enligt 5 kap. 1 § döms den som utpekar någon som brottslig eller klandervärd i sitt levnadssätt eller annars lämnar uppgift som är ägnad att utsätta denne för andras missaktning, för *förtal* till böter. Är brottet att anse som grovt döms enligt 5 kap. 2 § BrB för *grovt förtal* till böter eller fängelse i högst två år. Vid bedömningen av om brottet är grovt skall särskilt beaktas om uppgiften genom sitt innehåll eller den omfattning i vilken den har blivit spridd eller av annat skäl var ägnad att medföra allvarlig skada.

Uppgifter som sprids via Internet eller på en elektronisk anslagstavla torde normalt uppfylla kravet på omfattande spridning

Var gärningsmannen skyldig att uttala sig eller var det annars med hänsyn till omständigheterna försvarligt att lämna uppgift i saken, och visar han att uppgiften var sann eller att han hade skälig grund för den, skall ansvar för förtal inte utdömas.

Den som smädar annan genom kränkande tillmäle eller beskyllning eller genom något annat skymfligt beteende mot honom, döms, om gärningen inte är belagd med straff för förtal eller grovt förtal, för *förolämpning* till böter (5 kap. 3 § BrB). Är brottet grovt är straffet böter eller fängelse i högst sex månader.

Förtal och förolämpning får enligt huvudregeln inte åtalas av annan än målsägande (5 kap. 5 § BrB). Om målsäganden anger brottet till åtal och åtal av särskilda skäl anses påkallat ur allmän synpunkt får åklagare dock åtala för bl.a. förtal och grovt förtal, förolämpning mot någon i eller för hans myndighetsutövning eller förolämpning mot någon med anspelning på dennes ras, hudfärg, nationella eller etniska ursprung eller trosbekännelse. Utformningen av åtalsregeln innebär att det krävs mycket starka skäl för allmänt åtal och att presumtionen således är mot detta.

Bedömning

De befintliga straffbestämmelserna uppfyller kraven på kriminalisering i artiklarna 4 och 5. Det förhållandet att vissa brott endast får åtalas av målsägande torde sakna betydelse, vilket utvecklas närmare i det följande (avsnitt 7.5). Någon lagstiftningsåtgärd krävs därför inte.

Tryck- och yttrandefrihetsbrott

Hets mot folkgrupp tillhör sedan länge de brott som räknas upp i brottskatalogen i 7 kap. 4 § TF (p. 11). Detsamma gäller uppvigling, varigenom någon uppmanar eller annars försöker förleda till brottslig gärning (p. 10). Även förtal, varigenom någon utpe-

kar annan såsom brottslig eller klandervärd i levnadssätt eller annars lämnar uppgift som är ägnad att utsätta denne för missaktning, finns med i uppräkningen (p. 14). Straffansvaret omfattar även förtal av avliden. I katalogen ingår också förolämpning, varigenom någon smädar annan genom kränkande tillmäle eller beskyllning eller genom annat skymfligt beteende mot honom (p. 15).

Genom en lagändring, som har trätt i kraft nyligen (prop. 2001/02:74 s. 60), har TF:s brottskatalog utökats med bl.a. olaga hot (p. 16).

Sådant handlande som anges i 7 kap. 4 § TF kan, genom hänvisningen i 5 kap. 1 § YGL, även bestraffas som yttrandefrihetsbrott.

Regleringen i TF och YGL innebär att även brott enligt artiklarna 4 och 5 som begås i ett grundlagsskyddat medium kan beivras. Som tidigare nämnts lämna artikel 4 inget utrymme för förbehåll eller särskilda rekvisit, vilket däremot artikel 5 gör. I förhållande till artikel 5 bör övervägas möjligheten att göra förbehåll för att straffansvar inte utkrävs om detta skulle strida mot den svenska regleringen av yttrandefriheten. Det förhållandet att den svenska regleringen i vissa hänseenden innehåller avvikande regler har dessutom stöd i ingressen till protokollet, där det särskilt framhålls att protokollet inte avser att rubba etablerade principer på yttrandefrihetsområdet. Några lagstiftningsåtgärder krävs därför inte.

7.3.4 Förnekande, förringande och rättfärdigande av folkmord m.m. (artikel 6)

Bedömning: Reglerna om hets mot folkgrupp, uppvigling och ärekränkningsbrott innebär att kravet på kriminalisering i artikel 6 till stora delar är uppfyllt. Det som för närvarande faller utanför det straffbara området bör inte, av hänsyn till de grundläggande principerna bakom den svenska yttrandefriheten, kriminaliseras. Sverige bör i stället utnyttja möjligheten

att göra förbehåll. Något förslag till lagstiftning läggs därför inte fram.

Den svenska yttrandefriheten lämnar stort utrymme åt åsikter som för en bred allmänhet framstår som okunniga, felaktiga, olämpliga eller rentav motbjudande. Motmedlet mot sådana åsikter är möjligheten att i en fri och öppen debatt anföra motargument. Det råder stor politisk enighet om de unika värdena med den svenska öppenheten. Varje diskussion om en utvidgad kriminalisering av yttranden måste ta sin utgångspunkt i detta förhållande.

Artikel 6 innehåller krav på kriminalisering av gärningar som innebär att någon med hjälp av ett datorsystem sprider eller på annat sätt gör tillgängligt material som förnekar, grovt förringar, gillar eller rättfärdigar gärningar som utgör folkmord eller brott mot mänskligheten. Det finns inte någon direkt motsvarighet till detta brott i svensk rätt. En sådan gärning torde dock i många fall uppfylla rekvisiten för något av brotten hets mot folkgrupp, uppvigling eller för ärekränkningsbrott.

Uttalanden som innebär ett rättfärdigande eller gillande av folkmord eller brott mot mänskligheten torde i de allra flesta fall uppfylla rekvisiten för hets mot folkgrupp. Det är svårt att tänka sig något exempel där någon uppsåtligen gör sig till tolk för sådana åsikter utan att komma i konflikt med den straffbestämmelsen. Ett sådant uttalande kan också vara straffbart enligt någon av de andra bestämmelser som har nämnts tidigare. Den svenska lagstiftningen uppfyller således utan tvekan kraven på kriminalisering i artikel 6 i fråga om rasistiska och främlingsfientliga uttalanden som innebär gillande eller rättfärdigande av folkmord eller brott mot mänskligheten. Även uppsåtligt förringande kan i vissa fall, t.ex. om det har formen av förlöjligande, falla under vad som redan är straffbart.

Däremot kan det på goda grunder hävdas att en kriminalisering av andra fall av förnekande eller förringande av folkmord eller brott mot mänskligheten än vad som för närvarande är straffbelagt kommer i konflikt med bestämmelserna om yttran-

defrihet i RF. Enligt 2 kap. 12 § andra stycket RF får, som tidigare nämnts, begränsningar i yttrandefriheten göras enbart för ändamål som är godtagbara i ett demokratiskt samhälle. Den djupt rotade svenska traditionen på yttrandefrihetsområdet skiljer sig i många avseenden från motsvarande reglering i andra länder genom vår månghundraåriga vana vid öppenhet. Att vissa länder begränsar yttrandefriheten bl.a. när det gäller händelserna under andra världskriget måste också ses mot bakgrund av dessa länders deltagande i kriget. Det skulle emellertid strida mot grundvalarna för den svenska yttrandefriheten att, utöver vad som redan är kriminaliserat, förbjuda någon att ge till känna en åsikt om ett visst historiskt skeende, även om det är uppenbart att åsikten i fråga både är sakligt felaktig och har sådana inslag i övrigt att samhället tar starkt avstånd från den. Det kan därför inte anses vara ett godtagbart ändamål att i ett öppet samhälle som Sverige begränsa åsiktsfriheten på det sätt som skulle krävas för en fullständig kriminalisering i enlighet med artikel 6.

Härtill kommer att eventuella brott sannolikt i de allra flesta fall skulle komma att falla under det exklusiva utgivaransvaret i TF eller YGL.

Enligt artikel 6 punkt 2 har parterna rätt att ställa upp krav på att förnekandet eller förringandet görs med uppsåt att uppmana till hat, diskriminering eller våld mot en enskild individ eller en grupp av personer på grund av ras, hudfärg, härstamning, nationellt eller etniskt ursprung eller trosbekännelse. En part kan alternativt förbehålla sig rätten att, helt eller delvis, inte tillämpa artikeln.

Det generella undantaget i ingressen för etablerade principer om yttrandefrihet innebär att det inte kan krävas att Sverige inför straffrättsliga regler som motsvarar kraven i artikel 6 på det grundlagsskyddade området. Några sådana ändringar bör inte heller göras. Det är en etablerad svensk princip att inte förbjuda yttranden vilkas innebörd är att förneka eller förringa t.ex. förintelsen av judar, romer och andra grupper under andra världskriget.

De skäl som talar mot ändringar på det grundlagsskyddade området talar även med styrka mot en kriminalisering av sådant förnekande och förringande som äger rum med hjälp av datorer men som inte faller under den särskilda regleringen av tryck- och yttrandefrihetsbrott. Något förslag till lagstiftning läggs därför inte fram.

Sverige måste då förbehålla sig rätten att inte tillämpa den aktuella artikeln till den del den avser förnekande eller förringande av folkmord eller brott mot mänskligheten. Som framgått ovan finns det två alternativ. Alternativet i punkt 2 a med särskilt uppsåt skulle kräva ändringar i bestämmelsen om hets mot folkgrupp som tidigare har avvisats därför att de inte har ansetts förenliga med den svenska rättstraditionen på yttrandefrihetsområdet. Något skäl att nu ändra inställning i den frågan finns inte, eftersom undantag i stället kan göras enligt punkten 2 b. Sverige bör således avge förklaring att undantaget i artikel 6 punkt 2 b utnyttjas. Förbehållet bör för tydlighetens skull utformas så att det omfattar såväl gärningar utanför som inom det område som skyddas av TF och YGL. Frågan om förbehåll behandlas vidare i avsnitt 11.11.

7.3.5 Medhjälp (artikel 7)

Bedömning: Det behövs inte några lagstiftningsåtgärder för att uppfylla kraven i artikel 7.

Enligt artikel 7 skall uppsåtlig medhjälp till de brott som behandlas i tilläggsprotokollet vara straffbar.

Allmänna brott

Som framgått i avsnitt 6.8 skall enligt 23 kap. 4 § BrB straffansvar ådömas inte bara den som har utfört gärningen utan även den som har främjat denna med råd och dåd. Medverkansansvaret omfattar samtliga brott i brottsbalken samt straffbestämmel-

ser i andra lagar och författningar under förutsättning att fängelse är föreskrivet för brottet.

Regleringen i 23 kap. BrB av medhjälpsansvar täcker kraven i artikel 7 såvitt gäller allmänna brott.

Tryckfrihets- och yttrandefrihetsbrott

På grundlagsområdet gäller som huvudregel att endast den ansvarige utgivaren kan åtalas, eller, om denne inte kan anträffas, nästa person i tur i den särskilda kedja av ansvariga som anges i lagstiftningen. Det finns därför inget utrymme för medverkansregler när det gäller tryck- och yttrandefrihetsbrott.

Ingresstexten innebär att det grundlagsreglerade området inte påverkas. Att Sverige inte uppfyller kraven på medhjälpsansvar i de fall där brotten är att bedöma som tryckfrihets- eller yttrandefrihetsbrott saknar därför betydelse. Någon lagstiftningsåtgärd är därför inte nödvändig.

7.4 Generella krav (del av artikel 8)

Bedömning: Det behövs inte några lagstiftningsåtgärder för att Sverige skall uppfylla de generella kraven på straffbestämmelsernas utformning och tillämplighet.

Som framgått tidigare (avsnitt 5.2.4) är det inte tillräckligt att det handlande som skall kriminaliseras enligt tilläggsprotokollet stämmer överens med straffbestämmelser i svensk rätt. Det krävs också att reglerna om domsrätt är tillräckliga, att juridiska personers ansvar är tillfredsställande reglerat samt att brotten har en sådan straffskala att det är möjligt att använda straffprocessuella tvångsmedel i den utsträckning som anges i konventionen.

Vad som har sagts i avsnitt 6.11 angående de svenska reglerna om domsrätt gäller även för de allmänna brott som regleras i tilläggsprotokollet. När det gäller tryck- och yttrandefrihetsbrott täcker den svenska regleringen inte ett lika brett område.

Detta torde emellertid sakna betydelse eftersom det är fråga om etablerade principer för yttrandefriheten. Några lagstiftningsåtgärder krävs därför inte.

Regleringen av juridiska personers ansvar täcker, som framgått av avsnitt 6.9, kraven i konventionen. Detta gäller även för tilläggsprotokollet i fråga om allmänna brott. I fråga om tryck- och yttrandefrihetsbrott gäller, som framgått tidigare, särskilda ansvarsregler. Några lagstiftningsåtgärder krävs dock inte på detta område av nyss angivna skäl.

I sammanhanget bör också nämnas regleringen i 29 kap. BrB. Där anges hur straff skall bestämmas i det enskilda fallet. Kapitlet innehåller bl.a. bestämmelser om omständigheter som anses försvårande eller förmildrande och som på grund av detta skall påverka straffvärdet. En omständighet av försvårande art är enligt 29 kap. 2 § punkt 7 om ett motiv för brottet har varit att kränka en person, en folkgrupp eller en annan sådan grupp av personer på grund av ras, hudfärg, nationellt eller etniskt ursprung, trosbekännelse, sexuell läggning eller annan liknande omständighet. Regleringen av försvårande omständigheter är generell, dvs. den kan tillämpas på alla typer av brott.

7.5 Processrättsliga regler (del av artikel 8)

Bedömning: Det behövs, utöver de lagändringar som föreslås som ett led i anpassningen till konventionen, inte några lagstiftningsåtgärder för att Sverige skall uppfylla åtagandena på det processrättsliga området.

Tilläggsprotokollet hänvisar till konventionen när det gäller kraven på straffprocessuella regler. Detta innebär att det beträffande de brott som behandlas tilläggsprotokollet ställs samma krav som beträffande brotten i artiklarna 2-11 i konventionen i fråga om rättssäkerhetsgarantier och möjligheterna att med straffprocessuella tvångsmedel och andra metoder säkra bevisning m.m.

De förslag till ändrade regler på processrättens område som läggs fram i det följande kommer att kunna tillämpas på de brott

som behandlas i tilläggsprotokollet, om det är fråga om allmänna brott.

Att TF och YGL innehåller särskilda regler på det processuella området innebär, som framhållits tidigare, inga problem eftersom Sverige har rätt att behålla avvikande regler som hänför sig till etablerade principer för yttrandefriheten. Några lagstiftningsåtgärder på grundlagsområdet krävs därför inte.

En särskild fråga är hur man skall se på det förhållandet att brotten i 5 kap. BrB i huvudsak är målsägandebrott och därmed följer delvis andra regler än brott som ligger under allmänt åtal. För det första kan eller bör målsägandebrott normalt inte bli föremål för allmänt åtal. För det andra kan straffprocessuella tvångsmedel och andra metoder som hör hemma i en förundersökning inte annat än undantagsvis användas vid målsägandebrott. För det tredje har dessa brott en straffskala som är betydligt lägre än för de övriga brott som nu är aktuella. Frågan är om detta har någon betydelse för Sveriges möjligheter att uppfylla åtagandena i tilläggsprotokollet.

De handlanden som enligt konventionen skall vara straffbelagda torde normalt falla under andra straffbestämmelser än de som regleras i 5 kap. BrB, framför allt under reglerna om hets mot folkgrupp och olaga hot. Den kriminalisering som finns i dessa bestämmelser är tillräcklig för att Sverige skall uppfylla åtagandena i tilläggsprotokollet. Om det därutöver finns ytterligare regler som i och för sig täcker delvis samma område men som inte är lika långtgående torde vara av underordnad betydelse. Det finns därför ingen anledning att vidta några lagstiftningsåtgärder i fråga om brotten i 5 kap. BrB.

7.6 Internationellt samarbete (del av artikel 8)

Bedömning: Det krävs, utöver de lagändringar som föreslås som ett led i anpassningen till konventionen, inga lagstiftningsåtgärder för att Sverige skall kunna uppfylla åtagandena i tilläggsprotokollet om internationellt samarbete.

7.6.1 Rättslig hjälp

I fråga om rättslig hjälp hänvisar tilläggsprotokollet till artiklarna 23-35 i konventionen, som skall tillämpas även på protokollet.

Allmänna brott

Vad som har sagts i avsnitt 6.13.1 angående rättslig hjälp gäller även för nu aktuella brott.

Tryck- och yttrandefrihetsbrott m.m.

Nuvarande reglering

Lagen om internationell rättslig hjälp är, enligt vad som uttalades i förarbetena, inte tillämplig på det tryck- och yttrandefrihetsrättsliga området (prop. 1999/2000:61 s. 73). Det innebär bl.a. att Sverige inte kan erbjuda rättslig hjälp i de fall där brottet är att betrakta som ett tryckfrihets- eller yttrandefrihetsbrott.

JK har vidare påpekat att en åklagare inom åklagarväsendet inte torde kunna bistå andra länders myndigheter med rättslig hjälp i fråga om gärningar som faller inom TF:s och YGL:s tillämpningsområden (prop. 2001/02:74 s. 93). Detta beror på att JK är ensam behörig åklagare i fråga om sådana brott.

Frågan om reglerna om internationell rättslig hjälp bör omfatta även det tryck- och yttrandefrihetsrättsliga området berördes flyktigt i nyssnämnda proposition. Regeringen ansåg att det kunde finnas anledning att överväga om bestämmelserna bör ses över, för att Sverige i större omfattning än för närvarande skall kunna bistå med rättslig hjälp inom det tryck- och yttrandefrihetsrättsliga området. Sådana överväganden borde dock göras i annat sammanhang (a. prop. s. 93).

En oundviklig konsekvens av att den nuvarande regleringen inte omfattar rättslig hjälp vid tryckfrihets- och yttrandefrihetsbrott är att hjälp inte kan lämnas enligt bl.a. artiklarna 29 och 30 (snabbt säkrande och utlämnande av datorlagrad information

samt röjande av trafikuppgifter), om det är fråga om brott inom det grundlagsskyddade området.

Förslag till ändringar

Regeringen tillsatte under år 2003 en beredning på det tryck- och yttrandefrihetsrättsliga området. I direktiven till denna ingick bl.a. att överväga om möjligheterna att lämna rättslig hjälp inom det tryck- och yttrandefrihetsrättsliga området skall utökas. Uppdraget omfattade även att överväga om möjligheten att vidta andra åtgärder inom ramen för rättslig hjälp, t.ex. att besluta om utlämning och verkställighet av utländska domar, kan utökas i fråga om TF:s och YGL:s tillämpningsområden.

Tryck- och yttrandefrihetsberedningen har nyligen avgett ett delbetänkande som behandlar nu nämnda frågor; Vissa tryck- och yttrandefrihetsrättsliga frågor (SOU 2004:114). Beredningen konstaterar inledningsvis att det inte finns något underlag för en säker uppfattning om hur stort problem det är att rättslig hjälp inte kan lämnas vid tryck- och yttrandefrihetsbrott. Från senare år är endast sju fall kända där avslag har meddelats på grund av att det varit fråga om sådana brott.

Beredningen konstaterar vidare att det är oklart i vilken utsträckning som rättslig hjälp kan lämnas och att det därför är angeläget att rättsläget klarläggs (SOU 2004:114 s. 153 ff).

Det står enligt beredningen samtidigt klart att det i Sverige finns en s.k. vit makt-miljö i vilken det produceras skivor och annat material med rasistiskt innehåll vilket sedan sprids till andra delar av världen (a.a. s. 120 f).

Beredningen föreslår att en ny regel om internationellt rättsligt bistånd införs i 14 kap. TF och att en hänvisning till denna regel tas in i 11 kap. YGL. Regleringen innebär att internationellt rättsligt bistånd i vissa fall kan lämnas när TF eller YGL är tillämplig på det yttrande, meddelande eller anskaffande som ligger till grund för begäran om hjälp. Bistånd skall då kunna lämnas utan hinder av att svensk rätt föreskriver en särskild processordning i TF resp. YGL. Bistånd skall också kunna lämnas i fråga

om en gärning som utgör brott mot utländsk lag och som motsvarar ett brott mot någon av de bestämmelser som avses i 1 kap. 8 och 9 §§ om bl.a. upphovsrätt. Enligt förslaget skall de vanliga reglerna om internationell rättslig hjälp tillämpas, vilket innebär att det är åklagare inom åklagarväsendet som ansvarar för handläggningen. Innan hjälp lämnas skall dock JK alltid yttra sig. I fråga om politiska brott får hjälp lämnas endast efter medgivande av regeringen.

Enligt beredningens förslag skall möjligheterna att lämna rättslig hjälp begränsas till fall där enligt svensk lagstiftning ett straffrättsligt ingripande mot det aktuella brottet är möjligt. Det innebär krav på dubbel täckning, dvs. att brottet både ingår i TF:s brottskatalog och är straffbart enligt lag, samtidigt som kravet på dubbel straffbarhet i förhållande till den stat som begär rättslig hjälp upprätthålls. Det särskilda systemet för hantering av tryck- och yttrandefrihetsbrott kommer således, om förslaget genomförs, att även fortsättningsvis sätta gränser för möjligheterna att ge rättslig hjälp.

Beredningen föreslår vidare att tillägg görs i 14 kap. 6 § andra stycket TF och i 10 kap. 2 § YGL, för att det skall stå klart att en förutsättning för att skyddet för meddelande respektive anskaffande till medier som inte ges ut här i landet skall gälla är att meddelandet eller anskaffandet skedde här. Genom tillägget klarläggs att internationellt rättsligt bistånd kan lämnas enligt vanliga regler när det är fråga om meddelande eller anskaffande utomlands.

Bedömning

Framställningar om rättslig hjälp kan förväntas bli vanligare när det internationella samarbetet har utvecklats i fråga om gärningar som behandlas i konventionen om IT-relaterad brottslighet. Det gäller inte minst i fråga om brott som behandlas i tilläggsprotokollet. Detta innebär att man har anledning att räkna med ett ökande antal ansökningar som rör brott som i Sverige omfattas av det tryck- och yttrandefrihetsrättsliga systemet.

Frågan om utrymmet för att lämna rättslig hjälp vid tryck- och yttrandefrihetsbrott skall utökas har, som framgått ovan, nyligen utretts. Betänkandet kommer att bli föremål för remissbehandling.

Om en utveckling sker i enlighet med de förslag som har lagts fram av Tryck- och yttrandefrihetsberedningen förbättras Sveriges möjligheter att bistå andra länder med rättslig hjälp vid tryck- och yttrandefrihetsbrott. En sådan utveckling framstår som önskvärd. Eftersom både konventionen och tilläggsprotokollet ger utrymme för att avslå framställningar om rättslig hjälp om ett bifall skulle strida mot den anmodade statens allmänna rättsprinciper utgör emellertid den nuvarande regleringen inget hinder mot att Sverige, redan innan den frågan är avgjord, ansluter sig till tilläggsprotokollet.

7.6.2 Utlämning m.m.

Allmänna brott

Vad som har sagts i avsnitt 6.13.2 angående utlämning och överlämnande gäller även för nu aktuella brott.

Tryck- och yttrandefrihetsbrott m.m.

Frågan om det är förenligt med gällande rätt att besluta om utlämning för tryck- eller yttrandefrihetsbrott har också utretts av Tryck- och yttrandefrihetsberedningen (se SOU 2004:114 s. 82 ff). Beredningen fann att för rättsligt bistånd i denna form gäller samma begränsningar som för annat rättsligt bistånd. Den särskilda regleringen av tryck- och yttrandefrihet torde således utgöra hinder mot utlämning som grundas på en gärning som i Sverige omfattas av TF eller YGL.

Som redovisats i föregående avsnitt finns det emellertid redan ett förslag om att rättslig hjälp i ökad utsträckning skall kunna lämnas för sådana brott. Det förslaget omfattar även utlämning.

Den nuvarande regleringen utgör, som tidigare framhållits, inget hinder mot anslutning till tilläggsprotokollet redan innan statsmakterna har hunnit ta ställning till det nyssnämnda förslaget. Detta har sin grund i det generella undantag för etablerade principer till skydd för yttrandefriheten som finns i ingressen till protokollet.

7.7 Övriga bestämmelser (artiklarna 1-2 och 9-16)

Bedömning: Övriga delar av konventionen kräver inte någon anpassning av den svenska lagstiftningen.

Artiklarna 1 och 2 innehåller inga krav på anpassning av den nationella rätten.

Slutbestämmelserna i tilläggsprotokollet bygger på samma principer som konventionen. Dessa kräver inte några lagstiftningsåtgärder.

7.8 Slutsatser angående lagstiftningsbehovet

Bedömning: Det krävs inga lagstiftningsåtgärder för att uppfylla åtagandena i tilläggsprotokollet, om förbehåll görs för del av artikel 6. Även i fråga om artiklarna 3 och 5 bör övervägas förbehåll för särregleringen i fråga om tryck- yttrandefrihetsbrott.

Som framgått ovan behövs det inga lagstiftningsåtgärder för att uppfylla åtagandena i tilläggsprotokollet i fråga om straffbestämmelser, om förbehåll görs för del av artikel 6. Sverige bör även i övrigt göra förbehåll för den särreglering som finns på yttrandefrihetsområdet.

Det finns inte heller något behov av ändringar av de processrättsliga reglerna, utöver vad som har angetts i avsnitt 6.12 och som är en konsekvens av själva konventionen.

Utöver vad som har sagts i avsnitt 6.13 finns det inte heller något behov av lagstiftningsåtgärder för att uppfylla åtagandena om internationellt samarbete i tilläggsprotokollet.

8 Läget i andra länder i fråga om införandet av konventionen m.m.

8.1 Allmänt om arbetet med att genomföra konventionen

8.1.1 Europarådets uppföljning

När konventionen öppnades för undertecknande i november 2001 anslöt sig ett stort antal stater till denna. Anslutningen kom härigenom att bli mycket stor redan från början. Den fortsatta utvecklingen har emellertid varit långsammare. CDPC sammanställde i mars 2004 resultaten av en enkät angående hur arbetet med att genomföra konventionen om IT-relaterad brottslighet fortskrider i medlemsstaterna. Redovisningen i det följande bygger bl.a. på dessa uppgifter.

Inom ramen för Europarådets Octopus Programme, som är ett särskilt program mot korruption och organiserad brottslighet, hölls en konferens i Strasbourg i mitten av september 2004, i syfte att påskynda arbetet med ratifikation och genomförande av konventionen. Då hade konventionen nyligen trätt i kraft sedan det föreskrivna minimiantalet stater hade ratificerat denna. Vid avslutningen av konferensen framhöll Europarådets generalsekreterare vikten av dels att så många stater som möjligt över hela världen ansluter sig till konventionen, dels att de som har undertecknat konventionen ratificerar denna så snabbt som möjligt. Inom Europarådet övervägs möjligheten att ytterligare följa upp processen med ratificering i de enskilda medlemsländerna.

8.1.2 De nordiska länderna

De övriga nordiska länderna har, i likhet med Sverige, undertecknat Europarådets konvention om IT-relaterad brottslighet. Med undantag av Norge har dessa har även undertecknat tilläggsprotokollet till konventionen. Vid utgången av år 2004 hade inget nordiskt land ännu hunnit ratificera konventionen. Arbetet med att genomföra den lagstiftning som krävs har, som redovisas närmare i det följande, hunnit olika långt.

I samtliga länder synes det framför allt vara den del av konventionen som innehåller krav på anpassning av den nationella rätten och då särskilt processrätten som bereder bekymmer, medan frågan om att tillträda konventionen synes vara mera okontroversiell. I det följande lämnas en kort redogörelse för arbetet i de övriga nordiska länderna. De danska respektive norska lagstiftningsprojekten, som har hunnit längst, redovisas mera i detalj.

Det bör emellertid betonas att det är svårt att göra några direkta jämförelser mellan de övriga nordiska ländernas lagstiftning och den svenska, eftersom lagstiftningen skiljer sig åt i fråga om detaljer. Detta gäller framför allt på det processrättsliga området.

8.1.3 Övriga länder

Konventionen har undertecknats av flertalet stater som är medlemmar i Europarådet. Vid utgången av år 2004 hade 34 av medlemsstaterna undertecknat konventionen. Något färre (23 stater) hade undertecknat tilläggsprotokollet. Vidare hade fyra icke medlemsstater (USA, Kanada, Japan och Sydafrika) undertecknat konventionen. Ingen av dessa hade dock undertecknat tilläggsprotokollet.

8.2 Förhållandena i de nordiska länderna

8.2.1 Danmark

Danmark undertecknade konventionen den 22 april 2003.

I november 2003 lade justitieministern fram förslag om ändringar i strafflagstiftningen, processlagstiftningen, marknadsföringslagen och upphovsrättslagen. Förslagen byggde dels på förslag från en kommitté (Brydensholt-udvalget) som hade till uppgift att behandla frågan om i vilken utsträckning som utvecklingen på IT-området gjorde det nödvändigt med nya straffbestämmelser eller ändring av gällande regler, dels på överväganden inom justitiedepartementet angående vilka ändringar som krävdes för att Danmark dels skulle kunna ratificera konventionen dels genomföra EU:s rambeslut om angrepp mot informationssystem. Det danska lagstiftningsarbetet utmynnade i korthet följande.

För att uppfylla kraven i artiklarna 2-4 och 8 i konventionen om IT-relaterad brottslighet krävs det inga lagändringar. Den befintliga lagstiftningen täcker dessutom de flesta av de förfaranden som skall kriminaliseras enligt artiklarna 5 (dock inte hindrande av informationssystems funktion), 6 (dock inte tillhandahållande av åtkomstkoder och liknande), 9 och 10. För att bättre möta kraven i artikel 10 bedömdes vissa ändringar i upphovsrättslagen vara nödvändiga. I fråga om artikel 9 (barnpornografibrott) ansågs det att Danmark borde använda möjligheten till reservation i artikel 9 fjärde stycket.

Artikel 7 (dataförfalskning) bedömdes kräva mer omfattande ändringar. En generell anpassning av lagstiftningen på det sättet att elektroniska dokument och bevis jämställs med handlingar av traditionellt slag föreslogs. Reglerna om förfalskning föreslogs ändrade på det sättet att begreppet dokument skall omfatta en skriftlig eller elektronisk handling. Dokumentet skall i båda fallen ha en utställare som avger en utsaga som framstår som avsedd att tjäna som bevis (§ 171 i straffeloven). Den straffbestämmelse som reglerar skyldigheten att lämna korrekta uppgifter i offentliga dokument, vissa intyg samt böcker och liknande som förs på

grund av en rättslig eller annan förpliktelse (§ 175 i straffeloven) skulle på motsvarande sätt göras tillämplig på såväl elektroniska som traditionella dokument. Det skulle också införas en ny bestämmelse om förfalskning av elektroniska pengar (§ 169 i straffeloven).

Bestämmelsen om skadegörelse (§ 291 i straffeloven) skulle ändras bl.a. på det sättet att bland försvårande omständigheter skall beaktas om gärningen är av mera systematisk eller organiserad natur.

En ny bestämmelse (§ 301 a i straffeloven) skulle införas, som föreskriver straffansvar för den som olovligen skaffar sig eller lämnar vidare koder eller andra åtkomstverktyg till informationssystem, till vilka åtkomsten är förebehållen betalande användare, och vilka är skyddade med hjälp av koder eller andra åtkomstbegränsningar. Straffet föreslogs bli böter eller fängelse i högst ett år och sex månader och vid särskilt försvårande omständigheter högst sex års fängelse.

Vidare föreslogs vissa ändringar i syfte att få strafflagstiftningen mera teknikneutral, bl.a. på det sättet att begreppet databehandlingsanläggning skulle bytas ut mot uttrycket informationssystem.

Straffskalorna för IT-relaterade brott sågs över allmänt, varvid framför allt bestämmelser som tidigare haft en låg straffskala (t.ex. hacking) föreslogs få en strängare sådan. Härigenom skulle straffprocessuella tvångsmedel kunna användas i större utsträckning än tidigare för IT-relaterade brott.

Danmark anpassade redan år 1999 sin lagstiftning för att bättre tillgodose kraven på utredning av IT-relaterade brott. Någon ändring behövdes därför inte för att uppfylla flertalet av konventionens krav på det processuella området. Vissa ändringar ansågs dock nödvändiga.

Det föreslogs att det i retsplejeloven införs ett helt nytt straffprocessuellt tvångsmedel. Under en förundersökning skulle enligt förslaget polisen få förelägga någon som tillhandahåller eller telenät eller teletjänster (dvs. teleoperatörer) att företa ”hastesikring” av lagrade elektroniska data, däribland trafikdata. Ett

sådant föreläggande skall innehålla uppgift om vilka data som skall säkras och under vilken period. Enligt samma bestämmelse skulle teleoperatörer åläggas att lämna ut de lagrade uppgifterna. Vägran att rätta sig efter föreläggandet skulle bestraffas med böter. Juridiska personer skulle också kunna åläggas ansvar.

Lagförslaget godtogs av folketinget och ändringarna trädde i kraft den 1 juli 2004.

Danmark avser att avge reservation i fråga om artikel 20 (upptagning av trafikdata; jfr artikel 14).

Tilläggsprotokollet undertecknades den 11 februari 2004. Från det danska justitiedepartementet har det upplysts att en ratifikation av tilläggsprotokollet inte torde kräva någon lagändring, mot bakgrund av att Danmark avser att göra förbehåll enligt artikel 3 tredje stycket, artikel 5 andra stycket b och artikel 6 andra stycket b.

Arbetet med ratifikation av såväl konventionen som tilläggsprotokollet har påbörjats.

8.2.2 Finland

Finland undertecknade konventionen den 23 november 2001.

Den finska lagstiftningen om informations- och kommunikationsbrott är i huvudsak från mitten av 1990-talet och innehåller därför straffbestämmelser som tar sikte på modern brottslighet. Det finns t.ex. en straffbestämmelse om kränkning av kommunikationshemlighet (38 kap. 3 § strafflagen). I bestämmelsen kriminaliseras bl.a. att någon obehörigen, genom att bryta ett säkerhetsarrangemang eller med någon annan sådan teknisk metod, skaffar uppgifter om ett meddelande som har upptagits elektroniskt och som är skyddat mot utomstående. Detsamma gäller om någon obehörigen skaffar uppgifter om innehållet i samtal, telegram, text-, bild- eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller om avsändande eller mottagande av ett sådant meddelande. Det finns även ett grovt sådant brott (38 kap. 4 § strafflagen). Strafflagen innehåller vidare en bestämmelse om dataintrång. Den straffbe-

lägger bl.a. att någon gör bruk av en användaridentifikation som han inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen tränger in i ett datasystem där data behandlas, lagras eller överförs elektroniskt (38 kap. 8 § strafflagen).

Justitieministeriet tillsatte under år 2002 en arbetsgrupp vars uppgift var att bereda godkännandet av konventionen. Arbetsgruppen överlämnade den 3 juni 2003 sitt betänkande, som innehöll förslag till ny lagstiftning. Betänkandet har remitterats. Remissvaren har sammanställts och materialet har publicerats i april 2004. En regeringsproposition är under utarbetande. Materialet finns endast tillgängligt på finska och det har därför inte varit möjligt att ta del av detta. Däremot kommer propositionen så småningom att översättas till svenska.

Enligt vad som har upplysts från justitieministeriet är det framförallt anpassningen av den nationella rätten på det processrätträttsliga området som har visat sig vara besvärlig.

Tilläggsprotokollet undertecknades den 28 januari 2003. Det finns för närvarande inga planer beträffande protokollet.

8.2.3 Island

Island undertecknade konventionen den 23 november 2001 och tilläggsprotokollet den 28 januari 2003. Den isländska lagstiftningen innehåller endast en paragraf som behandlar databrott, nämligen strafflagens § 228 punkt 1 som straffbelägger att någon på olagligt sätt skaffar sig åtkomst till datorbehandlade uppgifter eller datorprogram.

Den permanenta kommittén för straffrätt har fått i uppdrag att överväga behovet av lagstiftningsändringar för att konventionen skall kunna ratificeras. Det finns inte någon direkt tidsplan för arbetet, men uppgiften är enligt vad som har upplysts från justitiedepartementet högt prioriterad. Arbetet med att anpassa den straffrättsliga lagstiftningen har enligt uppgift inte inneburit några större svårigheter hittills, medan det är mera osäkert vilka svårigheter som anpassningen av den processrättsliga regleringen

medför. Förslagen kommer senare att beredas vidare inom justitiedepartementet.

Arbetet med tilläggsprotokollet, som också har anförtrotts åt kommittén, kommer att påbörjas senare.

8.2.4 Norge

Norge undertecknade konventionen den 23 november 2001. Den norska lagstiftningen hade redan tidigare anpassats så att den överensstämde väl med Europarådets rekommendation R 89 (9) om IT-relaterad brottslighet.

En kommitté (Datakrimutvalget) fick i uppdrag att föreslå de lagstiftningsändringar som krävs för en ratifikation av konventionen. Kommittén lämnade ett delbetänkande den 4 november 2003 (Lovtiltak mot datakriminalitet; NOU 2003:27). Betänkandet innehöll endast förslag till sådana ändringar som ansågs absolut nödvändiga för att en ratificering av konventionen skulle vara möjlig.

Strax före årsskiftet förelades Stortinget en proposition, som byggde på Datakrimutvalgets förslag (prp. 2004-2005 nr 40). I propositionen föreslås det dels att Norge ratificerar konventionen, dels de lagändringar som krävs för detta.

De föreslagna lagändringarna innebär i korthet följande.

Något förslag till utvidgning av bestämmelsen om dataintrång (§ 145 i straffeloven) läggs inte fram. Datakrimutvalget förutsätts dock arbeta vidare med vissa frågor i anslutning till bestämmelsen. Det anses inte heller vara nödvändigt med några lagändringar för att uppfylla kraven i artiklarna 3-5, 7-8 samt 10-14.

Däremot föreslås en ny straffbestämmelse som skall täcka kraven i artikel 6. Förslaget skall ses mot bakgrund av att den norska strafflagstiftningen innehåller få bestämmelser om förberedelse till brott. Enligt lagförslaget (§ 145 b i straffeloven) straffbeläggas att någon utan att ha rätt till det framställer, anskaffar, innehar eller gör tillgängligt password eller andra data som kan ge åtkomst till ett datorsystem eller dataprogram eller

annat som är särskilt ägnat att användas vid brott mot data eller datorsystem. Straffet är böter eller fängelse upp till sex månader eller bådadera. Vid grovt brott är straffet fängelse upp till två år. Medverkan är straffbar.

Frågan om bestämmelserna om barnpornografibrott uppfyller konventionskraven har behandlats i en särskild proposition (se nedan).

När det gäller den processrättsliga delen föreslås, för att uppfylla kraven i artikel 16, en ny bestämmelse i straffeprocessloven (§ 215 a). Bestämmelsen ger åklagare rätt att, som ett led i en förundersökning, förelägga en person att säkra elektroniskt lagrade data som kan antas ha betydelse som bevis. Föreläggandet skall gälla för viss tid, högst 90 dagar. Föreläggandet kan förlängas. Om säkrandet sker på begäran av annan stat skall det gälla i minst 60 dagar. Den mot vilken föreläggandet riktas skall på begäran lämna ut de trafikdata som är nödvändiga för att spåra varifrån de data som omfattas av föreläggandet kom och vart de sändes. Bestämmelsen innehåller också regler om underrättelse till den misstänkte.

Vidare förslås en ändring av straffskalan för dataintrång för att i större utsträckning göra det möjligt att använda straffprocessuella tvångsmedel.

För att uppfylla kraven i artikel 19 punkt 4 föreslås en ny regel i straffeprocessloven (§ 199 a), som ålägger var och en som har befattning med ett datorsystem skyldighet att lämna uppgifter som underlättar verkställigheten av husrannsakan. Bestämmelsen får inte användas mot den som är misstänkt.

Det föreslås också att Norge avger reservation i fråga om artikel 20 (upptagning av trafikdata i realtid; jfr artikel 14) samt förklaringar till artiklarna 2, 24, 27 och 29 punkt 4.

Norge har, som tidigare nämnts, inte undertecknat tilläggsprotokollet. Datakrimutvalget skall även överväga frågor rörande vilket lagstiftningsbehov som tilläggsprotokollet innebär. Arbetet påbörjades under hösten 2004.

I en proposition till Stortinget (prp. 2004-2005 nr 37) föreslås det ändringar i regleringen av straffansvaret för barnpornografi-

brott. Straffansvaret för sådana brott skall i fortsättningen regleras i en särskild bestämmelse i straffeloven (§ 204 a) i stället för att utgöra en del av den allmänna bestämmelsen om befattning med pornografi. Syftet med en särskild straffbestämmelse är bl.a. att tydliggöra att skildringar av barnpornografi oftast är ett övergrepp på barnet i fråga. Vidare utvidgas straffansvaret så att även anskaffning av barnpornografi nämns uttryckligen i straffbestämmelsen. För att också täcka in viss nedladdning av Internetfiler som inte i rättspraxis har bedömts utgöra straffbart innehav utvidgas straffansvaret till att planmässigt ”göre sig kjent med” barnpornografi. Tanken har inte varit att lägga straffansvar på den som tillfälligt stöter på barnpornografi vid surfning på Internet, eller som får sådant material nedladdat i sin dator utan att ha för avsikt att skaffa sig barnpornografi. Straffansvaret skall däremot drabba personer som vid upprepade tillfällen eller med viss planmässighet tar del av barnpornografi. Med de föreslagna ändringarna, som delvis har andra motiv än kraven i konventionen, uppfylls kraven i konventionens artikel 9.

8.3 Läget i några andra länder

8.3.1 Länder som har ratificerat konventionen

Konventionen hade vid utgången av år 2004 ratificerats av följande åtta stater: Albanien, Kroatien, Estland, Ungern, Litauen, Rumänien, Slovenien och den forna jugoslaviska republiken Makedonien.

Litauen och Ungern har båda gjort vissa förbehåll samt avgett deklarationer angående vissa artiklar. Estland och Rumänien har avgett deklarationer angående vissa artiklar. Övriga stater har inte gjort några förbehåll eller avgett några deklarationer i samband med ratifikationen.

Som tidigare har nämnts trädde konventionen i kraft den 1 juli 2004, då kravet på att minst fem stater (varav minst tre medlemsstater) skulle ha ratificerat denna uppnåddes. I förhållande till Albanien, Kroatien, Estland, Ungern och Litauen trädde kon-

ventionen i kraft denna dag. I förhållande till Rumänien trädde konventionen i kraft den 1 september 2004 och i förhållande till Slovenien och den forna jugoslaviska republiken Makedonien den 1 januari 2005.

8.3.2 Länder som inte har ratificerat konventionen

Medlemsstater i Europarådet

I flertalet medlemsstater inom Europarådet som har undertecknat men inte ratificerat konventionen pågår arbete med att genomföra denna.

I *Tyskland* pågår arbetet med att utarbeta förslag till den lagstiftning som krävs för att kunna ratificera konventionen. Det finns planer på att en ratifikation skall kunna komma till stånd någon gång under loppet av den innevarande riksdagsperioden, vilken löper ut i september 2006.

Enligt uppgift bereder den straffrättsliga delen av konventionen inga större bekymmer, medan det torde krävas betydligt flera förändringar av processrätten. Vilka ändringar som krävs är ännu inte färdigutrett.

Den preliminära bedömningen är att om konventionen ratificeras så behövs det inte några större förändringar för att kunna ratificera även tilläggsprotokollet.

I *Frankrike* tillämpas två ratifikationsprocedurer. Stadiet med att anpassa den nationella lagstiftningen på olika punkter pågår. Viss straffrättslig lagstiftning har redan ändrats. Enligt de preliminära bedömningarna kommer Frankrike att behöva avge reservationer på flera punkter, bl.a. i fråga om artikel 9 andra stycket (barnpornografibrott) samt artiklarna 21 (upptagning av innehållet i telemeddelanden) och 22 (jurisdiktion). Man räknar även med att avge reservation enligt artikel 6 i tilläggsprotokollet.

Österrike har successivt genomfört olika förändringar inom straffrätten. Genom ändringar år 2002 uppfylldes kraven i artiklarna 2-7 och genom en ändring den 1 maj 2004 uppnåddes även överensstämmelse med kraven i artikel 9. Däremot pågår fortfa-

rande arbetet med frågan om straffansvar för juridiska personer (artikel 12).

Icke medlemsstater

Ingen av de icke medlemsstater som har deltagit i utarbetandet av konventionen har ännu ratificerat denna.

I *USA*, som har varit pådrivande i arbetet med konventionen, krävs det inga lagändringar för ratifikation. Enligt uppgift har presidenten nu överlämnat frågan om ratificering till kongressens representanthus. Frågan har tidigare underställts senaten, som i ett utlåtande har ställt sig positiv. Någon tidsplan för ratificering finns inte.

9 Tillträde till konventionen

Förslag: Sverige skall ratificera Europarådets konvention om IT-relaterad brottslighet och tilläggsprotokollet till denna.

Sverige undertecknade den 23 november 2001 Europarådets konvention om IT-relaterad brottslighet. Som framgår av kapitel 8 har övriga nordiska länder och flertalet EU-länder också undertecknat konventionen. Detsamma gäller tilläggsprotokollet till konventionen. Ett intensivt arbete med att genomföra konventionen pågår i dessa länder. Det pågår även annat internationellt arbete i syfte att uppnå en effektivare bekämpning av brott som begås med hjälp av modern teknik. Ett exempel på detta är rambeslutet om angrepp mot informationssystem (se avsnitt 6.2.1 och 10).

Den ökade datoranvändningen inom i stort sett alla sektorer av samhället har lett till en ökad sårbarhet i fråga om angrepp riktade antingen mot datorsystemen som sådana eller mot uppgifter lagrade i datorsystem. Sådana angrepp kan ta sig olika former. En typisk form är angrepp som syftar till att förstöra informationen eller att störa datorsystem. Som exempel kan nämnas datavirus. Datavirus är gjorda för att själva kunna sprida sig vidare. En typ av sådan ”ohyra” som drabbar datorer är s.k. maskar, som i dag är den vanligaste formen av virusangrepp. Maskar sprider sig själva vidare till andra datorer, t.ex. genom att utnyttja de adresslistor som finns i den drabbade datorns system för elektronisk post. En vanlig smittväg för maskar och andra datavirus är via bilagor till elektronisk post eller via webbsidor som har infekte-

rats. Varje gång ett nytt datavirus upptäcks måste det skapas skydd i form av antivirus mot viruset i fråga.

Under senare år har det blivit allt vanligare med virusangrepp. Ett större sådant angrepp för något år sedan var viruset Loveletter som spreds via elektronisk post över hela världen. Under sensommaren 2003 iscensattes det enligt uppgift hittills mest omfattande angreppet mot datorvärlden genom masken Sobig.f. Angreppet, som snabbt spred sig globalt, krävde omfattande motåtgärder från både myndigheter, dataföretag och säkerhetsföretag. Det är inte klarlagt hur stora skador Sobig.f orsakade eller vilka motiv som låg bakom angreppet. Masken Sasser spreds under år 2004. Spridningen gick mycket snabbt och enbart detta virus uppges ha vållat skador hos företag, myndigheter och privatpersoner för miljarder euro.

En annan typ av angrepp är s.k. trojanska hästar. Trojanska hästar, som inte är synliga för datoranvändaren, består av koder som är gömda i vanliga program En trojansk häst kan t.ex. användas för att vid senare tillfälle utnyttja den drabbade datorn för datorbrottslighet. Den kan också användas för att spionera på den angripna datorn.

Det förekommer även angrepp vilkas syfte är att hindra datorsystem från att fungera normalt, bl.a. s.k. tillgänglighetsattacker (Denial of Service-angrepp). En sådan attack kan exempelvis innebära att informationssystem avsiktligt överbelastas genom meddelanden som skapas automatiskt. Program som skapar och sänder så stora mängder elektronisk post att mottagarens system blockeras är ett exempel. Sådana angrepp kan åstadkommas även genom manuella sändningar i stor skala. Det kan också vara fråga om att genom upprepade kontakter blockera ett datorsystem för andra användare. Syftet med en tillgänglighetsattack kan t.ex. vara att tillfälligt sätta en affärskonkurrent ur spel eller att demonstrera mot en myndighets eller ett företags verksamhet. Det kan också vara att åstadkomma en så kraftig överbelastning att den dator som är målet förstörs. Utomlands har det även förekommit att sådana attacker har iscensatts i utpressningssyfte.

Det förekommer även kombinationer av de nu nämnda huvudtyperna av angrepp. Som exempel kan nämnas viruset NOVAR.G, även kallat MyDoom. Enligt uppgift var det fråga om ett virus som spreds via bilagor till elektronisk post. När viruset infekterar en dator öppnas samtidigt en hemlig s.k. bakdörr till datorn. Den gör att datorn senare tillfälligt kan ”tas över” av en hacker. Syftet med detta påstås vara att hackern med hjälp av de drabbade datorerna vill iscensätta massiva tillgänglighetsattacker riktade mot ett visst företag.

Det är emellertid inte bara datavirus och attacker av nyssnämnda slag som utgör hot. Dataintrång kan också resultera i att en hacker får kontroll över vitala samhällsfunktioner, som t.ex. informationssystem som styr verksamheten vid en flygplats, en kraftanläggning, en dammanläggning eller någon annan liknande anläggning. Nödsystem som styrs elektronisk kan sättas ur funktion genom dataintrång. Vidare kan sådana intrång resultera i att sekretessbelagda uppgifter blir åtkomliga.

Oavsett om datorangrepp riktar sig mot systemen som sådana eller mot de lagrade uppgifterna kan de, med dagens höga datorberoende, snabbt leda till svåra ekonomiska och/eller praktiska konsekvenser.

Den moderna tekniken utnyttjas också som ett medel vid olika typer av traditionella brott. Det förekommer t.ex. angrepp mot bankers och andra finansiella institutioners datorsystem, där syftet med angreppet kan vara att lura systemet att göra felaktiga utbetalningar eller överföringar. Betalning sker i allt större utsträckning i elektronisk form, vilket har banat väg för nya typer av förmögenhetsbrott riktade mot enskilda och företag. Barnpornografi och andra förbjudna alster sprids ofta via Internet. En annan brottstyp där datoranvändning numera spelar en viktig roll är brott mot upphovsrättslagen som består i olovlig kopiering och spridning av upphovsrättsligt skyddade alster. Vidare utnyttjas Internet för att beställa narkotika, dopingmedel och andra förbjudna varor från andra länder. De nu angivna brottstyperna är bara exempel som belyser varför undersökning av datorer, spårande av elektronisk kommunikation samt bevisning i

elektronisk form får allt större betydelse för brottsbekämpningen.

Det finns delade meningar om hur omfattande och allvarlig den IT-relaterade brottsligheten är i Sverige (se BRÅ-rapport 2000:2 s. 49 och SOU 2000:25 s. 178 och 208). Däremot råder det enighet om att den måste tas på allvar och att det krävs nya verktyg för bekämpning av sådan brottslighet. Konventionen utgör ett viktigt steg på vägen mot en effektivare bekämpning av brott där IT-teknik har kommit till användning.

Sverige har länge intagit en ledande position såväl i fråga om lagstiftning på IT-området som i fråga om hög grad av datoranvändning. Det är därför viktigt att Sverige har en strafflagstiftning som ger ett gott skydd mot missbruk av den moderna tekniken och en processlagstiftning som ger goda möjligheter att utreda IT-relaterade brott. Det är också viktigt att Sverige deltar aktivt i det internationella samarbetet med att bekämpa brottslighet av detta slag, eftersom ett utmärkande drag för denna är att den inte låter sig hejdas av gränser mellan länder. Mot den nu angivna bakgrunden bör Sverige ratificera konventionen och tillträda tilläggsprotokollet.

Samtidigt är det viktigt att värna om grundläggande värden i det svenska rättssystemet. Vad som är särskilt viktigt i detta sammanhang är den vidsträckta yttrandefrihet och frihet att söka information var helst den finns som är inskriven i den svenska grundlagen. Rätten till skydd för den personliga integriteten (bl.a. skyddet för personuppgifter och skyddet för förtroliga meddelanden) och värnandet om den enskildes rättssäkerhet är andra viktiga värden. Frågor av det slaget har haft en framskjuten roll vid utarbetandet av konventionen, vilket också framgår av ingressen till denna. Dessa frågor har i än högre grad präglat arbetet med tilläggsprotokollet. Det svenska intresset av att behålla öppenheten i samhället har härvid beaktats.

Konventionens bestämmelser bör, i likhet med andra överenskommelser av liknande slag, transformeras till svensk lag, dvs. omarbetas till svensk författningstext.

Sverige avgav inga reservationer vid undertecknandet av konventionen om IT-relaterad brottslighet. Inte heller avgavs några förklaringar om undantag från vissa artiklar. Detsamma gäller tilläggsprotokollet. Möjligheten att ange reservationer och undantag kvarstår emellertid fram till ratificeringen beträffande såväl konventionen som tilläggsprotokollet. Behovet av reservationer och undantag behandlas i avsnitt 11.11.

10 Rambeslutet om angrepp mot informationssystem

10.1 Innehållet i rambeslutet

Som tidigare har nämnts (avsnitt 6.2.1) har det utarbetats en promemoria med förslag till de lagändringar som behövs för att genomföra det av riksdagen godkända rambeslutet om angrepp mot informationssystem (Angrepp mot informationssystem; Ds 2005:5).

Rambeslutets artikel 1 innehåller definitioner. *Informationssystem* definieras som en apparat eller en grupp av sammankopplade apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas. Med *datorbehandlingsbara uppgifter* avses framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift. *Juridisk person* definieras som en enhet som har sådan status enligt tillämplig lagstiftning. Undantag görs dock för stater och andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt för internationella offentliga organisationer. Även begreppet *orättmätigt* definieras. Med orättmätigt avses ett handlande som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller en del av detta. Ett handlande är inte heller orättmätigt om det medges i nationell lagstiftning.

Av de nu nämnda definitionerna finns det motsvarigheter till definitionerna av informationssystem och datorbehandlingsbara uppgifter i konventionens artikel 1. Definitionerna i fråga är inte exakt likalydande men motsvarar i allt väsentligt varandra.

Enligt artikel 2 i rambeslutet skall medlemsstaterna straffbelägga handlande som utgör olagligt intrång i informationssystem, åtminstone i fall som inte är ringa. Bedömningen i promemorian är att den svenska lagstiftningen uppfyller kraven i artikeln, som i sak i huvudsak överensstämmer med artikel 2 i konventionen. I konventionen görs dock, som tidigare har nämnts, inget undantag för brott som är ringa. Det sistnämnda har betydelse för omfattningen av straffansvaret för försöksbrott.

Artikel 3 i rambeslutet behandlar olaglig systemstörning. Enligt denna artikel skall det vara straffbart att uppsåtligen och orättmätigt allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter. Artikeln har sin motsvarighet i artikel 5 i konventionen. Eftersom informationssystem enligt rambeslutet inte omfattar nät medan artikel 5 i konventionen även omfattar informationsintrång i nät finns det här en skillnad mellan rambeslutet och konventionen.

Enligt artikel 4 i rambeslutet, som rör olaglig datastörning, skall det vara straffbart att uppsåtligen radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, om gärningen utförs orättmätigt, åtminstone i fall som inte är ringa. Artikeln har sin motsvarighet i artikel 4 i konventionen.

Utöver de artiklar som nu har nämnts finns det inte några artiklar som behandlar kriminalisering i rambeslutet. Däremot finns det, i likhet med vad som är fallet med konventionen, krav på att anstiftan, medhjälp och försök till de gärningar som skall vara straffbelagda skall vara straffbar. I rambeslutet föreskrivs dessutom vilka påföljder som skall kunna dömas ut och vidare regleras försvårande omständigheter. Några motsvarigheter till detta finns inte i konventionen, som däremot innehåller krav på

kriminalisering av vissa andra gärningar, bl.a. olovlig avlyssning, dataförfalskning och databedrägeri.

Härutöver innehåller rambeslutet artiklar om ansvar och påföljder för juridiska personer och om jurisdiktion. I sak skiljer dessa sig inte särskilt mycket från motsvarande artiklar i konventionen.

10.2 Förslag till lagändringar för att genomföra rambeslutet

I promemorian om genomförande av rambeslutet konstateras det att det bara krävs ett fåtal författningsändringar, för att svensk lagstiftning skall stå i överensstämmelse med rambeslutet. Eftersom rambeslutet har mycket stora likheter med konventionen i fråga om de artiklar som rör kriminalisering redovisas i det följande huvuddragen i förslagen.

Promemorian utgår från att de lagstiftningsändringar som behövs för att uppfylla kraven på kriminalisering i rambeslutet skall göras i bestämmelsen om dataintrång. I promemorian analyseras bestämmelsen och dess nuvarande omfattning ingående. De bedömningar som görs angående behovet av lagändringar stämmer i sak överens med de bedömningar i fråga om motsvarande artiklar i konventionen som har gjorts i avsnitt 6.

I promemorian föreslås flera ändringar i bestämmelsen om dataintrång. För det första föreslås det att den som uppsåtligen och olovligen undertrycker en upptagning för automatiserad databehandling skall dömas för dataintrång. Den föreslagna ändringen föranleds av krav i rambeslutet som motsvarar kraven i konventionens artiklar 4 och 5 på att undertryckande av uppgifter skall vara straffbart.

För det andra föreslås att det införs straffansvar för den som uppsåtligen och olovligen på annat sätt allvarligt hindrar användningen av en upptagning för automatiserad databehandling. Den nu beskrivna ändringen föranleds av ett krav i rambeslutet som motsvarar det i artikel 5 i konventionen på straffansvar för allvarligt hindrande av ett datorsystems funktion.

Dessutom föreslås det vissa andra ändringar och förtydliganden i straffbestämmelsen. Det klargörs, genom en ändring av upptagningsbegreppet, att bestämmelsen om dataintrång omfattar alla uppgifter som befordras via elektroniska vågor och som är avsedda för databehandling, oavsett om befordran äger rum via ledningsbundna nät eller på annat sätt. Bestämmelsen moderniseras också genom att uttrycket automatisk databehandling ersätts med det numera använda uttrycket automatiserad databehandling.

Enligt promemorian bör förslaget till lagändring träda i kraft den 1 januari 2007.

10.3 Promemorians lagförslag

I promemorian om genomförande av rambeslutet föreslås det att bestämmelsen om dataintrång (4kap. 9 c § BrB) ändras på följande sätt.

Nuvarande lydelse	*Föreslagen lydelse*
Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för *automatisk* databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för dataintrång till böter eller fängelse i högst två år. Med upptagning avses *härvid* även uppgifter som *är under befordran* via *elektroniskt eller annat liknande hjälpmedel för att användas* för *automatisk* databehandling.	Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till *en* upptagning för *automatiserad* databehandling eller olovligen ändrar eller utplånar eller i register för in *en* sådan upptagning döms för dataintrång till böter eller fängelse i högst två år. *Detsamma gäller den som undertrycker eller på annat sätt allvarligt hindrar användningen av en sådan upptagning.* Med upptagning avses även uppgifter som *befordras* via *elektromagnetiska vågor och*

som är avsedda för *automatiserad* databehandling.

11 Förslag till lagändringar m.m.

11.1 Ändrade straffregler

11.1.1 Allmänt om behovet av straffrättsliga ändringar

Som framgår av avsnitt 6.1 täcker de nuvarande straffreglerna, framför allt bestämmelsen om dataintrång, i allt väsentligt de förfaranden som enligt konventionen om IT-relaterad brottslighet skall vara kriminaliserade som intrång i eller störning av datorsystem eller datorbehandlingsbara uppgifter. I vissa fall sträcker sig den svenska kriminaliseringen längre än vad konventionen kräver, något som konventionen inte hindrar. Det är därför bara på några få punkter som det krävs författningsändringar för att konventionens krav i fråga om artiklarna 2, 4 och 5 skall uppfyllas.

I kapitel 10 har redovisats hur det, som ett led i genomförandet av IT-rambeslutet, nyligen har föreslagits förändringar i regeln om dataintrång. Dessa förslag motsvarar nära nog helt de ändringar som krävs i den svenska lagstiftningen för att uppfylla konventionens krav på straffansvar för intrång i och påverkan på informationssystem och datorbehandlingsbara uppgifter (konventionens artiklar 2, 4 och 5).

Eftersom det redan finns ett förslag som tillgodoser behovet av lagändringar i nu aktuella hänseenden behandlas här enbart sådana frågor som inte tas upp i promemorian om genomförande av IT-rambeslutet, nämligen i vad mån ytterligare förändringar krävs för genomförandet av konventionen i dessa delar.

Förslagen i det följande tar således sin utgångspunkt i att regeln om dataintrång utvidgas och förändras på det sätt som har föreslagits i promemorian Angrepp mot informationssystem (Ds 2005:5). Utformningen av den föreslagna lagtexten framgår av avsnitt 10.

11.1.2 Bör bestämmelsen om dataintrång ändras i fler avseenden än vad som redan har föreslagits?

Bedömning: Det krävs inte några ändringar i bestämmelsen om dataintrång, utöver vad som redan har föreslagits som ett led i genomförandet av IT-rambeslutet, för att uppfylla kraven i konventionen på kriminalisering av gärningar som innebär intrång i eller påverkan på informationssystem eller datorbehandlingsbara uppgifter. Straffansvaret för försök och förberedelse till dataintrång bör inte utökas till att omfatta sådana brott som, om de hade fullbordats, skulle ha varit att bedöma som ringa. I stället bör Sverige utnyttja möjligheten att avge förbehåll.

Allmänt om förslagen

Den nuvarande bestämmelsen om dataintrång täcker inte helt det område som enligt konventionen skall vara straffbelagt när det gäller införing och undertryckande av uppgifter. Vidare saknas det straffrättsligt skydd mot gärningar som enbart hindrar ett datasystem från att fungera normalt. Frågan om avlyssning av datorer och datorsystem behandlas i avsnitt 11.1.3.

En konsekvens av att det här inte presenteras något förslag i fråga om de ändringsbehov som är gemensamma för genomförandet av IT-rambeslutet och konventionen om IT-relaterad brottslighet är att det krävs samordning av förslagen i det fortsatta lagstiftningsarbetet. Om det då skulle visa sig att genomförandet av IT-rambeslutet fördröjs av något skäl, krävs det att de i den promemorian föreslagna ändringarna i bestämmelsen om

dataintrång genomförs i det här lagstiftningsärendet, om Sverige skall kunna ratificera konventionen.

Olovlighetsrekvisitet

Konventionen förutsätter att handlande som sker orättmätigt skall straffbeläggas, medan regeln om dataintrång straffbelägger intrång och andra gärningar om de sker olovligen. IT-rambeslutet innehåller, som tidigare har redovisats, en definition av begreppet orättmätigt och analysen av om den svenska rätten uppfyller rambeslutets krav utgår från denna definition, som saknar motsvarighet i konventionen. En grundläggande fråga är således om olovlighetsrekvisitet i bestämmelsen om dataintrång uppfyller konventionens krav.

Ett intrång kan vara olovligt av olika skäl.

För det första kan det vara fråga om en helt olaglig åtgärd. Typiska exempel på detta är när en hacker tar sig in i någon annans dator eller när någon avsiktligt sprider datavirus till ett företags eller en myndighets datorsystem genom att sända ett elektroniskt meddelande.

För det andra kan det vara fråga om att någon handlar olovligt genom att överskrida sin behörighet eller sin befogenhet. Ett behörighetsöverskridande kan bestå i att någon som inte har systemägarens tillstånd att arbeta i ett visst datasystem lånar en åtkomstkod eller ett behörighetskort av någon annan som har denna behörighet. Ett vanligt exempel på befogenhetsöverskridanden är om en polisman, som i sig är behörig att hämta in uppgifter från brotts- och misstankeregistren, utnyttjar denna behörighet utöver vad som är tillåtet. Åtkomsten till uppgifter i registren begränsas nämligen av myndighetsföreskrifter som innebär att en polisman får ta del av uppgifter ur registren endast när det krävs för hans tjänsteutövning. Polismannen har således inte rätt att kontrollera om t.ex. en granne eller en rival finns i registren eftersom en sådan kontroll saknar anknytning till hans tjänst. Likaså har sjukvårdspersonal, som har tillgång till journalregister, på grund av föreskrifter endast rätt att ta del av journa-

ler som rör personer som de behandlar. Att ta del av andra patienters journaler är således inte tillåtet, men det förekommer. Befogenhetsöverskridanden av nu angivna slag är en av de vanligaste formerna av dataintrång.

För det tredje kan gärningen vara olovlig därför att gärningsmannen handlar i strid med samtycke eller avtal. Den som skall reparera eller uppdatera ett datasystem har givetvis systemägarens eller brukarens samtycke att vidta nödvändiga åtgärder för att genomföra sitt uppdrag, men om denne utnyttjar sin åtkomst till systemet till att vidta andra åtgärder – eller till att skaffa sig tillgång till delar av systemet som han inte har rätt att arbeta i – kan det vara fråga om ett olovligt intrång.

En åtgärd som annars är olovlig kan i det enskilda fallet vara lovlig, t.ex. på grund av samtycke, användning av straffprocessuella tvångsmedel eller regler om ansvarsbefrielse.

Som framgått av det sagda är olovlighetsrekvisitet i straffbestämmelsen om dataintrång komplext. Det täcker både otillåtna och olovliga förfaranden.

I konventionen används som tidigare har nämnts uttrycket ”orättmätigt” för att undanta sådana handlanden från straffansvar som objektivt sett skulle vara ett intrång om det inte fanns samtycke eller någon annan omständighet som gör åtgärden lovlig. Avsikten med uttrycket är just att det skall täcka gärningar som är otillåtna av olika skäl. Eftersom olovlighetsrekvisitet i sin nuvarande utformning uppfyller kraven i konventionen finns det inget skäl att ändra detta enbart av hänsyn till anpassningen till konventionen, vilket är samma bedömning som har gjorts i promemorian om genomförande av IT-rambeslutet.

Undertryckande av information

Enligt såväl artikel 4 som 5 skall det vara straffbart att undertrycka datorbehandlingsbara uppgifter. I promemorian om genomförande av IT-rambeslutet har det föreslagits ett tillägg till straffbestämmelsen om dataintrång som innebär att det skall vara straffbart att undertrycka en upptagning för automatiserad data-

behandling. Förslaget är utformat så att även kraven i konventionen uppfylls. Någon ytterligare lagändring krävs därför inte.

Data- och systemstörning

Ett område där den nuvarande kriminaliseringen är otillräcklig är i fråga om gärningar som påverkar ett datorsystems funktionalitet, det som även kallas data- eller systemstörning.

I promemorian om genomförande av IT-rambeslutet har det föreslagits en kriminalisering som innebär att den som – utan att bereda sig tillgång till, ändra, utplåna eller undertrycka en upptagning för automatiserad databehandling – på annat sätt allvarligt hindrar användningen av en sådan upptagning skall dömas för dataintrång. Så som bestämmelsen har utformats täcker den även införing som leder till sådan effekt. Förslaget uppfyller de återstående kraven på kriminalisering i konventionens artiklar 4 och 5. Någon ytterligare lagändring krävs därför inte.

Det kan i sammanhanget också nämnas att det har införts nya regler i marknadsföringslagen, vilka tar sikte på oönskad marknadsföring i form av obeställd e-postreklam (prop. 2003/04:43, bet. 2003/04:LU16). Ändringarna innebär att näringsidkare får använda elektronisk post för marknadsföring endast om den person som reklamen riktar sig till har samtyckt till det på förhand.

Försök och förberedelse

Artikel 11 punkt 2 i konventionen förutsätter att försök till brott enligt artiklarna 3-5 skall vara straffbara.

Enligt gällande rätt är försök till dataintrång straffbart, dock inte i de fall där brottet, om det hade fullbordats, skulle ha varit att anse som ringa. Motsvarande undantag gäller för förberedelse. Straffbestämmelsen om dataintrång är inte gradindelad. Det finns därför inte några klara riktlinjer för i vilka fall ett brott bör bedömas som ringa. Det finns inte heller någon rättspraxis som ger ledning i denna fråga.

IT-rambeslutet medger – i motsats till vad som är fallet med konventionen – generellt undantag för brott som är ringa. Frågan om man bör utvidga straffansvaret för brott som inte har fullbordats även till ringa brott har därför inte behandlats i promemorian om genomförande av IT-rambeslutet.

För att ett brott skall vara straffbart på försöksstadiet krävs det en särskild bestämmelse. Lagstiftaren har, i fråga om brotten i brottsbalken, i huvudsak valt att föreskriva sådant straffansvar bara för grova brott eller brott av normalgraden. Ringa brott är däremot normalt inte straffbelagda på försöksstadiet. Den avvägning av omfattningen av straffansvaret för försök som har gjorts i 4 kap. 10 § BrB motsvarar alltså vad som gäller i allmänhet i balken. Detta talar mot att utvidga straffansvaret för dataintrång till att omfatta även ringa brott. Det har inte heller framkommit några sakliga skäl för att göra undantag från den grundläggande strukturen i brottsbalken för just denna brottstyp. Sverige har möjlighet att behålla undantaget från det straffbara området för försök till ringa brott genom att avge förbehåll enligt artikel 11. Den lösningen framstår som den lämpligaste. Frågor om förbehåll behandlas vidare i avsnitt 11.11.

Straffvärdefrågor

Risken för IT-angrepp har ökat med den växande mängden datorer, den snabba utvecklingen av Internet-användning och det stora beroendet av fungerande datorsystem inom olika sektorer av samhället. Samtidigt är det relativt få fall av dataintrång som anmäls och utreds. Ännu färre blir föremål för domstolsbehandling. Den rättspraxis som finns är därför mycket begränsad. Mot den bakgrunden finns det inte någon anledning att nu ändra straffskalan för dataintrång, eftersom den uppfyller de krav som ställs i konventionen.

Däremot kan det finnas anledning att framhålla att vissa brott av det här slaget har ett betydande straffvärde. Det gäller särskilt brott som vållar betydande ekonomiska skador eller som av annat skäl ger särskilt kännbara effekter för dem som drabbas av

dem. Det finns därför anledning att noga följa utvecklingen i fråga om påföljder och straffmätning när ändringarna i straffbestämmelsen om dataintrång har trätt i kraft.

11.1.3 Olovlig avlyssning

Förslag: Olovlig avlyssning av datorer kriminaliseras. I bestämmelsen om dataintrång straffbeläggs att någon med tekniskt hjälpmedel olovligen avlyssnar elektromagnetiska emissioner eller andra icke allmänt tillgängliga signaler till eller från datorer eller datorsystem i syfte att få del av information. En särskild bestämmelse om förberedelse till sådan olovlig avlyssning införs också.

Vad skall kriminaliseringen omfatta?

Enligt artikel 3 skall det vara straffbart att med tekniska hjälpmedel orättmätigt avlyssna icke allmänna överföringar (däribland elektromagnetiska emissioner) av datorbehandlingsbara uppgifter till, från eller inom ett datorsystem. Konventionen ger möjlighet att för straffbarhet ställa krav på visst brottsligt uppsåt eller på att brottet skall begås mot ett datorsystem som är kopplat till ett annat.

När en dator arbetar ger den ifrån sig elektromagnetiska emissioner. Med detta avses att den oavsiktligt ger ifrån sig signaler som genom bearbetning kan omvandlas till information. Emissioner kan härröra såväl från maskinvaran som från kablar eller annan utrustning. Eftersom emissioner enligt konventionen inte faller under begreppet datorbehandlingsbara uppgifter nämns det särskilt att straffansvaret skall omfatta avlyssning av elektromagnetiska emissioner.

Det finns för närvarande inte någon straffbestämmelse som direkt tar sikte på avlyssning av datorsystem. Detta skall ses mot bakgrund av att det som regel krävs att någon gör sig skyldig till intrång i ett datorsystem för att kunna avlyssna den information

som finns i detta. Avlyssning av kommunikation mellan datorer som äger rum via allmänna kommunikationsnät faller under straffbestämmelsen om brytande av telehemlighet. Den klassiska formen av avlyssning, det som brukar kallas wiretapping, är således redan kriminaliserad. Vidare skyddas överföring av uppgifter som ännu inte har fixerats på ett datamedium genom utformningen av begreppet upptagning i bestämmelsen om dataintrång. Någon särskild straffbestämmelse om avlyssning av datorer har därför inte ansetts nödvändig.

Det nuvarande skyddet mot avlyssning av datorkommunikation bygger på den teknik som var förhärskande när skyddet tillskapades, dvs. trådbunden kommunikation. Utvecklingen har emellertid i stor utsträckning gått mot trådlös kommunikation. Numera är det t.ex. inte ovanligt med trådlösa datornätverk. Kommunikationen kan äga rum med hjälp av radiovågor, infrarött ljus eller via sattelit. Avlyssning av trådlösa nät faller utanför dagens straffbestämmelser, om det inte är fråga om ett intrång.

Ett annat exempel på hur tekniken har förändrat förutsättningarna för att tillämpa straffreglerna är en ny typ av datorhjälpmedel, nämligen den sladdlösa musen. I stället för att utnyttja en direkt koppling mellan musen och datorn sänder den sladdlösa musen informationen om användarens kommandon via radiovågor.

Möjligheterna att genom avlyssning snappa upp information från datorer och datorkommunikation torde ha ökat med teknikförändringar av de slag som nu har nämnts, samtidigt som straffskyddet inte är heltäckande.

Det kan visserligen hävdas att avlyssning av just sådan information som härrör från en sladdlös mus omfattas av den nuvarande straffbestämmelsen om dataintrång, eftersom den straffbelägger intrång som riktar sig mot uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel. Å andra sidan anses avlyssning av radiotrafik helt falla utanför det straffbara området för avlyssning (se prop. 1992/93:200 s. 166, bet. KU 1992/93:2 s. 18 och SOU 1992:110 s. 431). Det är nämligen en sedan länge vedertagen princip att etern är fri. Det står därför

var och en fritt att avlyssna såväl sådan radiokommunikation som är riktad till allmänheten som annan typ av radiokommunikation (se 6 kap. 17 § andra stycket 3 lagen om elektronisk kommunikation). En annan sak är att det i 6 kap. 23 § lagen om elektronisk kommunikation föreskrivs att den som via en radiomottagare har avlyssnat eller på annat sätt har fått tillgång till ett meddelande, som varken är avsett för honom eller för allmänheten, får inte obehörigen föra det vidare. Yppandeförbudet är straffsanktionerat (7 kap. 15 § första stycket lagen om elektronisk kommunikation). Detta förbud är dock, som framgår av lagtexten, begränsat till avlyssning med hjälp av radiomottagare.

Mot den nu angivna bakgrunden är det osäkert om avlyssning av radiosignaler från en sladdlös mus faller in under dagens bestämmelse om dataintrång, särskilt som det är en fråga som inte kan ha varit aktuell vid bestämmelsens tillkomst. Det är i så fall en lucka i den nuvarande bestämmelsen som har uppkommit till följd av ändrad teknik.

Det är således nödvändigt att utvidga straffansvaret för att kraven i artikel 3 skall uppfyllas. Om man enbart ser till konventionens krav torde man i princip kunna inskränka straffregelns tillämpningsområde till avlyssning av elektromagnetiska emissioner, eftersom de viktigaste formerna av annan avlyssning redan är straffbelagda. Straffansvaret är dock, som nyss har nämnts, inte heltäckande. Det går inte heller i dag att förutse den tekniska utvecklingen. Det kan inte uteslutas att det inom en nära framtid kommer att finnas andra möjligheter att snappa upp innehållet i datasystem och datorer utan direkt intrång. Utöver behovet av nykriminalisering som ett led i anpassningen till konventionen kan det därför även finnas andra skäl att överväga hur straffskyddet skall vara utformat.

En straffregel bör så långt möjligt vara teknikneutral. Det sagda talar för att straffansvaret i princip bör omfatta varje form av avlyssning av kommunikation till, från eller inom ett datorsystem. Mot detta talar emellertid att man inte i detta sammanhang bör ändra på den grundläggande principen om friheten att av-

lyssna radiokommunikation, särskilt som denna bygger på andra internationella överenskommelser.

Konventionen ställer inte något krav på att avlyssning av alla typer datainformation skall kriminaliseras utan endast sådan information som inte är allmänt tillgänglig. Regeln bör utformas i enlighet med detta. Härigenom kommer straffansvaret inte att omfatta radiosändningar och andra sändningar som är direkt avsedda för allmänheten. Inte heller sådana sändningar som visserligen inte är avsedda för allmänheten men som äger rum på ett öppet och lättåtkomligt sätt, och som därmed kan avlyssnas av var och en som har tillgång till en mottagare, träffas av straffansvaret. Exempel på det senare är radiokommunikation till sjöss.

Det kan finnas skäl att avgränsa kriminaliseringen ytterligare. Konventionen tillåter, som tidigare har redovisats, att det ställs särskilt krav på brottsligt uppsåt. Den möjligheten bör utnyttjas. För straffansvar bör krävas ett direkt uppsåt att genom avlyssningen olovligen skaffa tillgång till information. Ett sådant syfte torde kunna presumeras i de flesta fall där det kan påvisas att gärningsmannen har skaffat ett särskilt tekniskt hjälpmedel för att avlyssna datorutrustning, utom i de fall där anskaffandet har utgjort ett led i behörig testning av säkerheten. Har gärningsmannen tagit del av informationen är uppsåtskravet givetvis uppfyllt. Det kan emellertid ibland vara svårt att bevisa att så har varit fallet. Det bör därför räcka att gärningsmannen har haft tillgång till informationen i sådan form att han har kunnat tillgodogöra sig denna. Det saknar däremot betydelse om informationen har varit av något värde för gärningsmannen. Den kan t.ex. vara på ett språk som han inte behärskar. Något krav på att gärningsmannen också har haft uppsåt att använda informationen bör inte ställas upp. Även om informationen inte har varit läsbar eller på annat sätt omedelbart tillgänglig för gärningsmannen kan syftet, att olovligen skaffa information, således vara uppfyllt. Det kan ju även bero på teknisk oförmåga hos denne att han inte har kunnat tillgodogöra sig informationen.

Nykriminaliseringen bör, i likhet med regeln om olovlig avlyssning av samtal, endast omfatta avlyssning med tekniska

hjälpmedel. Den som i smyg tar del av informationen i ett datorsystem enbart genom att läsa på en bildskärm som en oförsiktig användare exponerar gör sin inte skyldig till brott enligt den föreslagna bestämmelsen.

Vidare skall det krävas att avlyssningen sker olovligen. Avlyssning som äger rum med samtycke eller som på någon annan grund är lovlig ligger därmed utanför det straffbara området. Härigenom kommer exempelvis sådan avlyssning som utgör ett inslag i kontrollen av säkerheten i ett datorsystem att falla utanför.

Det bör också betonas att regeln inte tar sikte på otillåten användning av dekoderutrustning. Dels är det fråga om utsändningar som är riktade till allmänheten, dels finns det särskilda straffregler för detta i lagen (2000:171) om förbud beträffande viss avkodningsutrustning.

Var skall regeln placeras?

En särskild fråga är var den nya straffbestämmelsen om olovlig avlyssning skall placeras. En möjlig lösning är att utvidga tillämpningsområdet för dataintrång. Vad som talar för den lösningen är att avlyssning av signaler från en dator eller från ett hjälpmedel som kommunicerar med datorn liknar andra förfaranden som kriminaliseras i straffbestämmelsen om dataintrång, eftersom det är ett av flera tänkbara sätt att olovligen bereda sig tillgång till information som datorbehandlas. Förfarandet har emellertid även stora likheter med bestämmelsen om olovlig avlyssning. En annan möjlighet är därför att utvidga det kriminaliserade området för olovlig avlyssning. Vad som talar för den lösningen är framför allt att syftet med att avlyssna ett datorsystem eller en dator inte behöver vara att påverka informationen eller systemen. Det kan t.ex. vara enbart nyfikenhet som ligger bakom avlyssningen.

Reglerna om dataintrång respektive olovlig avlyssning har samma straffskala. Ur det perspektivet spelar det således ingen

roll i vilken av paragraferna som den nya straffbestämmelsen placeras.

Försök till olovlig avlyssning är, i motsats till dataintrång, inte straffbart. Däremot finns det en särskild straffbestämmelse om förberedelse till olovlig avlyssning som straffbelägger anbringandet av tekniska hjälpmedel avsedda för avlyssning. Det sistnämnda talar för att man placerar en ny regel om avlyssning av datorer i den paragraf som reglerar olovlig avlyssning.

Om bestämmelsen placeras i 9 a § uppkommer å andra sidan frågan om konkurrens i förhållande till bestämmelsen om dataintrång. Som tidigare har nämnts täcker sistnämnda bestämmelse sådan avlyssning som utgör ett led i ett intrång. Så bör vara fallet även i fortsättningen. Detta kan i och för sig lösas genom att den nya bestämmelsen görs subsidiär i förhållande till bestämmelsen om dataintrång, men man får då en komplicerad inbördes relation mellan bestämmelserna där de ömsevis är subsidiära.

Vid en samlad bedömning talar övervägande skäl för att även olovlig avlyssning av datorsystem regleras i bestämmelsen om dataintrång.

Systematiken i straffbestämmelsen

Bestämmelsen om dataintrång är komplicerad genom att den täcker in såväl intrång i som störning av datorsystem. Det har emellertid betydande fördelar att reglera dessa förfaranden i samma straffbestämmelse. Bestämmelsens tillämpningsområde kommer att utvidgats om förslagen till ändringar i promemorian om genomförande av IT-rambeslutet genomförs. I den promemorian har gjorts bedömningen att bestämmelsen inte bör delas upp på olika brott så att den följer rambeslutet i detta avseende. Detta ställningstagande ter sig välmotiverat. Det kan tillfogas att konventionen har en delvis annorlunda systematik än IT-rambeslutet och att, om man vill dela upp bestämmelsen, det då kan ifrågasättas vilken systematik som bör väljas. Härtill kommer att en uppdelning på olika brott skulle kunna leda till tillämpningssvårigheter eftersom ett intrång ofta resulterar i exempelvis ra-

dering eller ändring. En sammanhållen reglering i en paragraf är därför att föredra.

Även med denna utgångspunkt tål det emellertid att diskuteras om straffbestämmelsen om dataintrång kan ges en något mer pedagogisk och lättillämpat utformning, t.ex. genom en indelning i punkter. Den frågan kan emellertid lämpligen tas upp i det fortsatta beredningsarbetet, varför något sådant förslag inte läggs fram här.

Osjälvständiga brottsformer

Straffansvaret skall enligt konventionen (artikel 11 punkt 2) även omfatta försök till olovlig avlyssning. I svensk rätt har generellt valts en annan lösning för att komma till rätta med osjälvständiga brottsformer vid informationsintrång, nämligen att straffbelägga som förberedelse att någon anbringar ett hjälpmedel som är avsett för avlyssning (9 b §). Skälet till att denna lösning valdes var att det ansågs vara svårt att bevisa att avlyssnings- och inspelningsapparatur som påträffas under sådana omständigheter, att man kan utgå från att den som har anbringat den har haft uppsåt att i hemlighet spela in eller avlyssna andras samtal, verkligen har använts för detta ändamål.

En motsvarande lösning bör väljas för att uppfylla konventionskravet på ansvar för försök till olovlig avlyssning av datorsystem. Det blir emellertid av lagtekniska skäl nödvändigt att reglera detta brott i en särskild paragraf. Med den valda lösningen uppfylls kravet på ansvar för försök till olovlig avlyssning i artikel 11 punkt 2.

11.1.4 Dataförfalskning

Bör urkundsbegreppet ändras?

Förslag: Det nuvarande urkundsbegreppet, som har vital betydelse för reglerna i 14 kap. BrB, bör inte ändras.

I artikel 7 i konventionen behandlas förfalskning av elektroniska data. Vad som skall kriminaliseras är att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter så att det uppstår icke autentiska uppgifter. Syftet skall vara att dessa uppgifter skall beaktas eller ligga till grund för handlande i rättsliga hänseenden som om de vore autentiska. Det spelar ingen roll om uppgifterna är direkt läsbara och begripliga. Artikeln har, som tidigare nämnts, ingen direkt motsvarighet i nuvarande lagstiftning.

I svensk rätt bygger reglerna om förfalskning på urkundsbegreppet, som är centralt för förfalskningskapitlet (se avsnitt 6.3). När bestämmelsen om dataintrång tillkom ansågs det självklart att en maskinellt framställd handling kunde utgöra en urkund (prop. 1973:33 s. 145), om den i övrigt uppfyllde kraven för urkunder. I rättspraxis fäster man således inte något avseende vid på vilket tekniskt sätt en handling har framställts, så länge den uppfyller de allmänna krav som ställs på en urkund. Som exempel kan nämnas ett avtal eller någon annan handling som har framställts i en persondator men sedan omvandlats till en vanlig pappershandling som har undertecknats.

Så länge en text eller en sammanställning av siffror enbart finns i digital form uppfyller den däremot inte annat än i undantagsfall de kriterier som ställs på ett förfalskningsobjekt (se avsnitt 6.3.2). Urkundsbegreppet utgår nämligen från traditionella sätt att framställa skrift och låter sig svårligen förenas med hur den moderna tekniken fungerar innan innehållet i en datorframställd text har fixerats och fått en fysisk form. Tidigare förslag om att anpassa urkundsbegreppet till IT-tekniken har inte lett till lagstiftning. Man måste således skilja mellan elektroniskt framställda handlingar som har materialiserats i annan form och handlingar som enbart förekommer i elektronisk form.

Under senare år har man börjat tala om elektroniska urkunder (se exempelvis Statskontorets rapport 2003:13). Med detta avses elektroniska originalhandlingar försedda med någon typ av elektronisk underskrift. Regler om elektroniska signaturer finns i lagen (2000:832) om kvalificerade elektroniska signaturer. Med

elektronisk signatur enligt 2 § denna lag avses data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats. En avancerad elektronisk signatur är enligt samma paragraf knuten enbart till en undertecknare, som är möjlig att identifiera. Signaturen är dels skapad med hjälpmedel som endast undertecknaren kontrollerar, dels knuten till andra elektroniska data på sådant sätt att förvanskning av dessa data kan upptäckas. I lagen definieras även kvalificerade elektroniska signaturer, som är skapade av en säker anordning för signaturframställning och som anses uppfylla krav i lag eller annan författning på egenhändig underskrift eller motsvarande.

Åtminstone sådana elektroniska urkunder som är försedda med en avancerad eller kvalificerad elektronisk signatur torde kunna jämställas med urkunder av traditionellt slag och därmed också kunna utgöra förfalskningsobjekt. Det är emellertid osäkert i vilken utsträckning man i övrigt kan dra paralleller mellan traditionella urkunder och elektroniska handlingar.

Även om det finns en bred kunskap om att ett elektroniskt framställt dokument inte kan tillmätas ”originalstatus” på samma sätt som ett dokument framställt med äldre teknik, spelar det förhållandet att de förstnämnda har samma förtroendeingivande utseende som en trycksak en roll. Trots att det i dag är tekniskt enkelt att efterlikna ett företags logotype eller en myndighets emblem uppfattas i många fall en elektroniskt framställd handling med sådana kännetecken som lika förtroendeingivande som en tryckt handling. Datorframställda handlingar har således allmänt sett ett förtroendeingivande yttre. Numera kan de även förses med en datorframställd ”namnteckning” som efterliknar en vanlig underskrift.

En elektroniskt framställd handling, som inte är försedd med en egenhändig underskrift (eller en motsvarande elektronisk signatur), har emellertid, lika lite som en icke vidimerad fotokopia, någon tydlig utställare. Den som får del av en sådan handling kan

inte vara säker på vare sig att innehållet är äkta eller att handlingen härrör från den som uppges vara utställare.

I viss utsträckning är emellertid förfalskning av elektroniska data straffbar. Straffansvaret för bedrägeri omfattar även den som genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, om gärningen innebär vinning för gärningsmannen och skada för någon annan. Att olovligen bereda sig tillgång till elektroniska data och ändra eller radera i dessa är straffbart som dataintrång. Det som bestraffas i sistnämnda fall är emellertid enbart intrånget, medan framställningen av falsk eller osann information inte i sig är straffbar.

Att lagtekniskt jämställa olovliga ändringar av elektroniska data med förfalskning av urkunder skulle leda till svåröverblickbara resultat. Det är t.ex. numera vanligt att texter sänds eller hämtas i elektronisk form. Detta skapar teknisk möjlighet att använda hela eller delar av texten i andra dokument eller att ändra, lägga till eller ta bort text från det ursprungliga dokumentet utan att ändringen syns på en utskrift eller kopia. Elektroniska dokument kan i och för sig förses med skydd mot bearbetning, som innebär att det syns om ändringar har gjorts, men den möjligheten utnyttjas långtifrån alltid. Vidare kan självfallet inte varje bearbetning av ett elektroniskt dokument betraktas som en förfalskning, även om den görs utan den ursprunglige upphovsmannens vetskap och vilja.

Att ändra – eller väsentligt utvidga – urkundsbegreppet enbart som ett led i anpassningen till konventionen ter sig alltså som ett alltför omfattande ingrepp. Överväganden angående hur användningen av modern teknik skall återspeglas i reglerna i 14 och 15 kap. BrB bör äga rum från ett bredare perspektiv än vad anpassningen till konventionen om IT-relaterad brottslighet erbjuder. En sådan översyn har också aviserats (se Ds 2003:29 s. 38). Inom Justitiedepartementet pågår arbetet med att utarbeta direktiv för översynen.

Det är inte heller nödvändigt med en så långtgående förändring för att kraven i konventionen skall kunna uppfyllas. Vad konventionen tar sikte på är straffansvar för att framställa, förändra eller undertrycka datorbehandlingsbara uppgifter så att det uppstår icke autentiska uppgifter. Härutöver krävs uppsåt att uppgifterna skall beaktas eller ligga till grund för handlande i rättsliga hänseenden som om de vore autentiska. I den förklarande rapporten (punkt 82) framhålls att den nationella rätten skiljer sig väsentligt mellan länderna, men att man kan se två huvudlinjer. Den ena (till vilken svensk rätt hör) utgår från utställaren. Den andra utgår från sanningshalten i innehållet. Minimikravet är att straffbestämmelsen skall täcka utställarens äkthet, men det står parterna fritt att låta kriminaliseringen omfatta även innehållets sanningshalt.

Mot bakgrund av den aviserade översynen bör väljas en lösning som uppfyller minimikraven i artikel 7 men som samtidigt i minsta möjliga utsträckning binder upp lagstiftningen för framtiden.

En annan lösning än ändring av urkundsbegreppet

Förslag: Straffansvaret för brukande av något som är förfalskat utvidgas till att omfatta åberopande av en icke autentisk sammanställning av elektroniska data, om den som åberopar denna ger sken av att den är autentisk. En förutsättning för straffansvar skall vara att åtgärden innebär fara i bevishänseende.

Utöver förfalskning av urkunder och förfalskning av vissa andra föremål (bl.a. mynt och sedlar, värde- och kontrollmärken) har i 14 kap. BrB straffbelagts att åberopa, begagna eller på annat sätt bruka något som är förfalskat, om åtgärden innebär fara i bevishänseende (14 kap. 9 § BrB). I subjektivt hänseende krävs uppsåt. För den som åberopar eller brukar något som är förfalskat tillämpas samma straffskala som om han själv hade utfört förfalskningen. Bestämmelsen fyller en viktig funktion i de fall där

det visserligen finns starka skäl att tro att någon har förfalskat en handling eller något annat förfalskningsobjekt men där detta inte kan bevisas. Använder han det förfalskade kan straffansvar i stället utkrävas för brukandet.

Ett elektroniskt framställt dokument skiljer sig från andra dokument genom att man inte på samma sätt som vid traditionella handlingar kan tala om original och kopior. En kopia av ett visst elektroniskt dokument blir exakt likalydande med en annan framställning av samma elektroniska data (prop. 1999/2000:117 s. 19). Däremot är texten, innan den har materialiserats t.ex. i form av en utskrift, som regel inte fixerad på sådant sätt att den inte kan ändras utan att det märks. Särskilt viktiga elektroniska upptagningar brukar dock förses med skydd mot bearbetning eller med markeringar av om texten har ändrats.

Som framgått tidigare torde det i många fall uppfattas som tillåtet att använda texter i elektronisk form för bearbetning, givetvis med beaktande av de gränser som bl.a. upphovsrätten sätter upp. Att generellt skapa ett skydd mot förändringar i elektronisk text framställd av annan framstår därför som verklighetsfrämmande. Det ställer sig annorlunda om texten i bearbetat skick utnyttjas för att ge sken av att den är en autentisk sammanställning av elektroniska data som härrör från en viss utställare när så inte är fallet. En lösning kan därför vara att utgå från att åberopande av icke autentiska elektroniska dokument skall straffsanktioneras på samma sätt som åberopande av förfalskade urkunder, när det sker uppsåtligen. Detta innebär att man utgår från syftet med gärningen, nämligen att den manipulerade sammanställningen skall användas och att den avses ligga till grund för att någon annan agerar som om det vore en äkta sammanställning.

Det kan naturligtvis diskuteras om en på detta sätt manipulerad sammanställning av data skall betraktas som falsk eller osann. En alternativ lösning kan nämligen vara att utvidga straffansvaret i bestämmelsen om missbruk av urkund, som finns i 15 kap. 12 § BrB. I den bestämmelsen straffbeläggs bl.a. att någon sanningslöst utger en handling, som har tillkommit genom genomslag

eller fotografering eller på annat dylikt sätt, för en riktig kopia av en urkund, om gärningen innebär fara i bevishänseende. Straffet för missbruk av urkund är böter eller fängelse i högst sex månader eller, om brottet är grovt, fängelse i högst två år. Försök och förberedelse till missbruk av urkund är inte straffbart.

En utvidgning av straffansvaret i bestämmelsen om missbruk av urkund skulle kräva en betydligt mer omfattande ändring av grundbestämmelsen. Denna har nämligen en väsentligt lägre straffskala än bestämmelsen om brukande av falsk urkund, vilket begränsar möjligheterna att använda straffprocessuella tvångsmedel. Vidare är det inte föreskrivet straff för osjälvständiga brottsformer. Straffskalan medför dessutom att brotten preskriberas snabbt.

Mot bakgrund av ställningstagandet att man bör göra minsta möjliga förändring i den befintliga lagstiftningen inför den aviserade översynen av reglerna om förfalskningsbrott och brott mot sanningsplikten är en lösning som innebär att man utvidgar straffansvaret för brukande av falsk urkund därför att föredra.

Vad som kan tala emot den valda lösningen är att det inte finns något förfalskningsbrott som den nya kriminaliseringen bygger vidare på. Detta torde dock inte vara något avgörande skäl mot att i nuläget göra den föreslagna förändringen. Om en framtida översyn leder till en ändrad syn på förfalskningsobjekten får den frågan övervägas på nytt.

Straffansvaret för brukande av falsk urkund bör alltså utvidgas till att omfatta åberopande av en icke autentisk sammanställning av elektroniska data. Med elektroniska data åsyftas detsamma som i lagen om kvalificerade elektroniska signaturer.

Frågan är om straffansvar bör kunna utkrävas även i de fall där det som åberopas senare har materialiserats i annan form än digital. Om så inte är fallet träffar ansvaret endast den som på en bildskärm visualiserar de förfalskade elektroniska uppgifterna eller som vidarebefordrar förfalskningen t.ex. i form av en datafil, en bilaga till elektronisk post eller överförd till en fysisk databärare som en diskett eller CD.

Att utvidga ansvaret utöver vad som oundgängligen krävs för att genomföra åtagandena i konventionen bör inte övervägas nu. Det bör således endast vara information i elektronisk form som träffas av kriminaliseringen.

För straffansvar bör krävas att åtgärden innebär fara i bevishänseende. Ett exempel på förfarande som kan falla under den nya straffbestämmelsen är om någon påstår att ett elektroniskt framställt dokument, som innehåller ett utlåtande i en sakfråga, härrör från en viss utställare, trots att så inte är fallet, och åberopar utlåtandet som om det vore äkta.

Eftersom försök till brukande av något som är förfalskat är straffbart uppfyller förslaget även kraven i artikel 11 punkt 2.

11.2 Övergripande processrättsliga frågor

11.2.1 Behovet av ändringar

Bedömning: Konventionens processrättsliga bestämmelser har ett mycket brett tillämpningsområde. De skall kunna tillämpas dels på de brott som anges i konventionens artiklar 2-11, dels på andra brott som har begåtts genom att gärningsmannen har utnyttjat datorteknik, dels på bevisning i elektronisk form i brottmål (oavsett brottstyp). Detta innebär att de processrättsliga reglerna måste anpassas med sikte även på utredningsformerna för andra brott än dem som omfattas av konventionens straffrättsliga del.

Det behövs inte några nya tvångsmedel för att tillgodose behovet av snabb tillgång till bevis i situationer där husrannsakan och beslag kan tillämpas. Det krävs emellertid vissa förändringar av regleringen rörande dessa tvångsmedel i de fall där bevisningen enbart finns i elektronisk form utan att ha lagrats på någon fysisk databärare. Bestämmelserna om edition behöver inte ändras för att tillgodose behovet av tillgång till information i elektronisk form. Däremot krävs det ändringar i reglerna om hemlig teleavlyssning och hemlig teleövervakning för att möta kraven i konventionen på skynd-

samt säkrande av bevisning. Det krävs också en helt ny reglering av sådant snabbt säkrande av bevisning som sker i samverkan med den som förfogar över lagrade data.

Dagens reglering uppfyller inte konventionens krav

Brott som begås med hjälp av datorer avsätter som all annan brottslighet spår, men dessa är av ett annat slag än de som förekommer vid traditionell brottslighet. Gärningsmannen kan i vissa fall befinna sig långt från platsen där brottet fullbordas och kan då som regel bara spåras genom datortrafiken.

Enligt 2 kap. 6 § RF är varje medborgare gentemot det allmänna skyddad mot bl.a. undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Detta skydd får enligt 2 kap. 12 § RF begränsas genom lag. En sådan begränsning får endast göras för att tillgodose ändamål som är godtagbart i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen.

En motsvarande reglering finns i Europakonventionen. Enligt artikel 8.1 har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten till skydd omfattar bl.a. överföring av meddelanden med hjälp av telefon, telefax, radio och datorkommunikation (Hans Danelius, Mänskliga rättigheter i europeisk praxis, 2002, s. 270). Denna rätt kan enligt artikel 8.2 begränsas med stöd av lag, bl.a. av hänsyn till den allmänna säkerheten och förebyggande av oordning eller brott.

Ett av de viktigaste problem som konventionen är avsedd att lösa är behovet av internationellt samarbete dels för att spåra pågående angrepp mot datorsystem (för att om möjligt begränsa skadeverkningarna), dels för att i efterhand kunna identifiera och lagföra gärningsmännen bakom sådana angrepp. Internationellt samarbete av detta slag förutsätter i sin tur att det finns effektiva möjligheter enligt den nationella rätten att få fram bevis om vilka

kommunikationsvägar som har använts för brottet och om vem som kan ligga bakom detta. Konventionen lämnar åt parterna att välja instrument för att uppfylla kraven i konventionen.

I svensk rätt görs ingen skillnad mellan olika typer av bevisning, annat än i fråga om hur bevisningen skall förebringas inför rätten. Bevis i elektronisk form särbehandlas således i princip inte. Detta innebär att det inte finns några legala begränsningar förknippade med bevisning i elektronisk form.

En annan sak är de rättsliga och praktiska förutsättningarna att med hjälp av straffprocessuella tvångsmedel få fram bevis i elektronisk form. Även om tvångsmedelsregleringen i princip inte gör skillnad mellan bevisning av olika slag, har det betydelse att vissa tvångsmedel syftar till att få fram muntlig bevisning medan andra syftar till att få fram skriftlig bevisning. Av större betydelse är emellertid att reglerna om reella tvångsmedel tillkom i en tid när bevis alltid hade en fysisk form. Tvångsmedlen är därför inte anpassade till dagens tekniska miljö, även om reglerna om vissa tvångsmedel successivt har moderniserats som en följd av den tekniska utvecklingen. Det har hittills inte heller ansetts nödvändigt att generellt ändra reglerna om reella tvångsmedel för att de skall passa IT-tekniken. Ett huvudskäl till detta är att dessa tvångsmedel i praktiken alltjämt i de flesta fall tillämpas på fysiska föremål. Anpassningen till konventionen ställer dock krav på vissa förändringar, vilket utvecklas närmare i avsnitt 11.6

Konventionen medför ett åtagande att införa regler om skyndsamt säkrande av bevisning i elektronisk form. Detta gäller såväl lagrade datauppgifter (artiklarna 16 och 17) som uppgifter om elektronisk kommunikation i realtid (artiklarna 20 och 21). I det senare fallet är det fråga om dels trafikuppgifter, dels uppgifter om innehållet i kommunikationen. Syftet med säkrandet är att uppgifterna skall bevaras under viss tid, för att senare kunna lämnas ut för brottsutredningsändamål. Vidare skall enskilda kunna åläggas att såväl bevara bevisning (artikel 16) som att lämna ut den (artikel 18). Svensk rätt uppfyller inte i alla delar konventionens krav.

Innan utgångspunkterna för förslagen läggs fast finns det skäl att erinra om att konventionens processrättsliga bestämmelser är avsedda att ha ett brett tillämpningsområde. De skall kunna användas dels för de brott som anges i konventionens artiklar 2-11, dels för andra brott som har begåtts genom att gärningsmannen har utnyttjat datorteknik, dels på bevisning i elektronisk form i brottmål oavsett brottstyp. Bevisning i elektronisk form blir allt vanligare, inte minst genom att polisens utredningsmetoder moderniseras. Som exempel kan nämnas brottsplatsundersökningar som dokumenteras med digitalkamera, fingeravtryckskontroll i digitala register och DNA-undersökning av spår. Konventionens breda tillämpningsområde innebär att de processrättsliga reglerna måste anpassas generellt och från ett vidare perspektiv än enbart konventionens straffrättsliga del.

Vad som för svensk del vållar särskilda problem vid anpassningen till konventionen är att elektroniska uppgifter som befordras av en teleoperatör (eller av någon annan som omfattas av regleringen i 6 kap. lagen om elektronisk kommunikation, men i fortsättningen används för enkelhetens skull enbart beteckningen operatör)[35] utgör telemeddelanden. Sådana är enbart åtkomliga genom reglerna om hemlig teleavlyssning och hemlig teleövervakning.

Innehållet i ett telemeddelande är uteslutande åtkomligt genom beslut om hemlig teleavlyssning. Tvångsmedlet kan vidare tillämpas bara för utredning av ett fåtal brottstyper eftersom det enligt huvudregeln krävs att det för brottet inte är föreskrivet lindrigare straff än fängelse i två år.

Uppgifter rörande ett visst telemeddelande, både trafikuppgifter och s.k. lokaliseringsuppgifter,[36] är i en brottsutredning åtkomli-

[35] Reglerna omfattar dels verksamhet som avser tillhandahållande av ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av ljudradioprogram eller annat som anges i 1 kap. 1 § tredje stycket YGL, dels tjänster inom ett allmänt kommunikationsnät som består av a/en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt eller b/en allmänt tillgänglig kommunikationstjänst till mobil nätanslutningspunkt. Beteckningen operatör används alltså i denna promemoria för att beteckna en vidare krets än vad definitionen i lagen om elektronisk kommunikation omfattar, nämligen den krets som omfattas av reglerna om tystnadsplikt m.m. i 6 kap. denna lag.

[36] Se avsnitt 11.8.3 angående begreppen trafikuppgifter och lokaliseringsuppgifter.

ga med stöd av reglerna om hemlig teleövervakning. Det ställs inte samma höga krav på straffskalan för hemlig teleövervakning. För brottet skall enligt huvudregeln inte vara föreskrivet lindrigare straff än fängelse sex månader.

Sådana uppgifter om telemeddelanden som finns lagrade hos operatören, och som avser annat än innehållet, kan i viss utsträckning även lämnas ut med stöd av lagen om elektronisk kommunikation (6 kap. 22 § första stycket 3). En förutsättning för detta är dock att det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, vilket innebär att samma krav ställs som för hemlig teleavlyssning.

Det är emellertid inte bara utformningen av tvångsmedelsreglerna som innebär begränsningar. Av hänsyn till den enskildes integritet är huvudprincipen att all information hos en operatör om elektronisk kommunikation skall utplånas eller avidentifieras så snart kommunikationen har avslutats, om inte uppgifterna behövs för vissa specificerade ändamål. Av dessa är debitering det praktiskt viktigaste. Vid användning av kontanttjänster eller andra tjänster (t.ex. flat rate) som inte kräver särskild debitering utplånas som regel uppgifterna snabbt, även om de sparas någon tid t.ex. för debitering av samtrafikavgifter. Det innebär att det kan vara en slump om uppgifterna är bevarade. Inom EU pågår emellertid arbetet med ett utkast till rambeslut, vars syfte är att utvidga operatörernas skyldighet att bevara uppgifter (se avsnitt 11.8.3).

Riksdagen har nyligen godkänt regeringens förslag till utvidgning av tillämpningsområdet för hemliga tvångsmedel (prop. 2002/03:74, bet. 2003/04:JuU2). Med verkan från den 1 oktober 2004 är även innehållet i sådan elektronisk kommunikation som till följd av avtal med abonnenten eller av annat skäl har lagrats hos en operatör åtkomligt, t.ex. meddelanden i en röstbrevlåda. Historiska uppgifter är åtkomliga i samma utsträckning som framtida uppgifter. Ändringarna innebär dock inte att operatörernas skyldighet att bevara uppgifter påverkas.

Hos en operatör får inte andra straffprocessuella tvångsmedel (t.ex. husrannsakan och beslag) eller edition användas för att få

fram uppgifter vars åtkomst exklusivt regleras i bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning (se avsnitt 6.12). Denna begränsning har för närvarande inte så stor praktisk betydelse, eftersom uppgifterna snabbt skall utplånas eller avidentifieras. Den har emellertid stor betydelse för frågan hur konventionsåtagandena skall överföras till svensk rätt.

Om uppgifter om viss telekommunikation finns hos någon annan än en operatör är informationen åtkomlig med vanliga tvångsmedel (husrannsakan och beslag). Så kan vara fallet t.ex. om mottagaren av ett telefonsamtal har spelat in detta och inspelningen finns bevarad, eller om abonnenten har fått en räkning (eller annan handling) med specificerade uppgifter om vilka teleadresser han har kontaktat och när kommunikationen har ägt rum. När uppgifterna finns hos mottagaren eller avsändaren av ett telemeddelande är detta meddelande inte starkare skyddat än exempelvis ett brev, som på samma sätt som ett telemeddelande har ett särskilt skydd så länge det är under befordran, medan det är åtkomligt med husrannsakan och beslag såväl innan det har avsänts som när det har nått sin adressat. Det är således förtroligheten vid befordran av meddelanden som åtnjuter särskilt skydd, inte handlingen eller innehållet i meddelandet som sådant. På motsvarande sätt förhåller det sig med spår av datakommunikation. För spår som finns hos någon annan än en operatör gäller vanliga tvångsmedelsregler.

Sammanfattningsvis kan sägas att det redan med nuvarande lagstiftning finns förutsättningar att hämta in elektroniska uppgifter som antingen är lagrade i en dator hos en brottsmisstänkt eller som har förts över till en fysisk bärare, t.ex. en diskett eller en CD. Vidare anses det möjligt att få fram elektronisk bevisning genom husrannsakan såväl hos den misstänkte som hos annan med stöd av reglerna i 28 kap. 1 § andra stycket RB. Uppgifter om telemeddelanden som finns hos en operatör kan dock, som nyss har nämnts, endast hämtas in tvångsvis med stöd av beslut om hemlig teleavlyssning eller hemlig teleövervakning. Den nuvarande ordningen med domstolsbeslut innebär att det inte är möjligt att tillräckligt snabbt säkra sådana uppgifter. Det finns

inte heller någon möjlighet att ålägga den som innehar bevisning i elektronisk form att samverka med brottsbekämpande myndigheter i syfte att säkra bevisningen.

Vilka principer bör gälla för den nya regleringen?

Den grundläggande synen i svensk rätt att bevisning av skilda slag i princip behandlas lika vid användning av tvångsmedel bör inte ändras vid anpassningen till konventionen. I stället bör lösningar väljas som knyter an till hur den nuvarande lagstiftningen om tvångsmedel är uppbyggd.

I de situationer där det redan nu finns möjlighet att snabbt ingripa med tvångsmedel för att säkra den efterfrågade bevisningen behövs inga förändringar. Såväl husrannsakan som beslag kan beslutas av åklagaren, annan förundersökningsledare och i brådskande fall även av en enskild polisman. Något behov av nya regler om tvångsmedel finns inte i de fall bevisningen omedelbart kan säkras genom husrannsakan och beslag. Däremot kan det behövas nya regler som gör det möjligt att temporärt förbjuda rubbandet av viss bevisning, för att skapa praktiska förutsättningar för att genomföra husrannsakan och beslag. Den frågan, liksom frågan om anpassning av reglerna om husrannsakan och beslag, tas upp i kommande avsnitt.

Det finns inte heller något skäl att frångå principen att hemlig teleavlyssning och hemlig teleövervakning skall vara de enda straffprocessuella tvångsmedel som får användas för att få fram uppgifter om telemeddelanden hos en operatör (se prop. 2002/03:74 s. 45 f). Det finns dock skäl att överväga om tillämpningsområdena för tvångsmedlen i fråga bör ändras. De nuvarande reglerna om hemliga tvångsmedel måste vidare ändras så att ett snabbare förfarande möjliggörs.

Det sagda innebär att förmedlingen av särskilt integritetskänsliga uppgifter kommer att ha ett fortsatt starkt skydd. Å andra sidan innebär det att man, i likhet med vad som redan nu är fallet, får en delvis olikartad tvångsmedelsreglering beroende på om uppgifterna finns hos en operatör eller hos någon annan.

I det nyss nämnda lagstiftningsärendet tog regeringen i lagrådsremissen upp Buggningsutredningens förslag om att avskaffa operatörernas skyldighet enligt lagen om elektronisk kommunikation att lämna uppgifter om annat än innehållet i ett telemeddelande. Förslaget syftade till att få bort dubbelregleringen i förhållande till rättegångsbalkens regler om hemlig teleövervakning. Detta förslag togs emellertid inte med i propositionen. Regeringen aviserade i stället en förnyad översyn av frågan (a prop. s. 12). Vid anpassningen till konventionen bör i första hand eftersträvas andra lösningar än att utvidga de nuvarande reglerna i lagen om elektronisk kommunikation om uppgiftslämnande till brottsbekämpande myndigheter. Skälet till detta är dels att den nu aktuella regeln om uppgiftslämnande är tillämplig endast på det fåtal brottstyper som kan ligga till grund för hemlig teleavlyssning, dels att det är osäkert om, och i så fall i vilken utsträckning, den möjligheten att inhämta uppgifter på sikt kommer att finnas kvar.

Bör editionsreglerna ändras?

Även edition kan aktualiseras som ett medel för att få tillgång till skriftliga bevis. Endast rätten kan besluta om edition, men edition förekommer sällan i brottmål eftersom reglerna om husrannsakan och beslag i princip är avsedda att ersätta editionsreglerna. Det finns dessutom legala begränsningar som medför att det praktiska utrymmet för att använda edition i brottmål är litet (se avsnitt 6.12.5).

Ibland begärs dock edition även i brottmål. Åklagaren kan yrka edition exempelvis för att få tillgång till allmänna handlingar (38 kap. 8 § RB). Vidare kan en målsägande yrka edition. Mot bakgrund av att edition sällan används i brottmål finns det inte något praktiskt behov av någon ny interimistisk åtgärd i förhållande till edition för att tillgodose kraven i konventionen på skyndsamt säkrande av bevis i brottmål.

Eftersom konventionen emellertid även godtar sanktioner som inte är av straffrättslig natur, exempelvis civilrättsliga åtgär-

der för att beivra intrång i upphovsrätt och närstående rättigheter, måste man ställa sig frågan om detta motiverar en annan bedömning av behovet av ändrade editionsregler.

För några år sedan infördes en ny tvångsåtgärd vid immaterialrättsintrång, s.k. intrångsundersökning (prop. 1998/99:11). Intrångsundersökning regleras i 56 a-h §§ upphovsrättslagen. Intrångsundersökning är en åtgärd som en rättighetsinnehavare kan begära inom ramen för ett civilrättsligt förfarande, för att säkra bevis hos någon som på goda grunder misstänks ha gjort intrång i en immateriell rättighet. Intrångsundersökning har stora likheter med husrannsakan, men beslut om sådan undersökning fattas av domstol på ansökan av rättighetsinnehavaren. Åtgärden verkställs av kronofogdemyndighet. Reglerna om intrångsundersökning tillgodoser behovet av att snabbt säkra bevis om upphovsrättsintrång utanför brottsmålsförfarandet. Någon ändring av editionsreglerna är därför inte heller av det skälet påkallad.

11.2.2 Utgångspunkter för förslagen

Bedömning: Man bör undvika skilda lösningar för olika typer av elektronisk kommunikation. Förslagen bör så långt möjligt bygga vidare på den befintliga lagstiftningen. Vidare bör teknikneutrala lösningar eftersträvas. Nya tvångsmedelsregler skall vara generella eftersom konventionen bygger på förutsättningen att de processrättsliga reglerna skall kunna användas i den nationella brottsbekämpningen.

En allmän utgångspunkt för de förslag som presenteras i det följande är att man bör undvika skilda lösningar för olika typer av elektronisk kommunikation. Ett huvudskäl till detta är att det i dag är omöjligt att förutse hur tekniken kommer att utvecklas i framtiden. Att binda tvångsmedelsreglerna till vissa typer av kommunikation eller vissa typer av teknik vore att ta ett steg tillbaka i utvecklingen. I stället bör man så långt som möjligt

bygga vidare på nuvarande regler. Man bör dessutom eftersträva teknikneutrala lösningar.

Konventionen bygger på förutsättningen att de processrättsliga reglerna skall kunna användas i den nationella brottsbekämpningen. Det är givetvis lika viktigt att kunna spåra en elektronisk kommunikation angående ett brott som utreds i Sverige som ett brott där svenska myndigheter endast bistår en annan stat med utredningsåtgärder. Lagstiftningen om internationell rättslig hjälp i brottmål utgår dessutom från att samma förfaranden skall användas vid rättslig hjälp som i en svensk förundersökning. Reglerna skall därför vara generella.

Övervägandena i det följande behandlar framför allt tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning (avsnitt 11.3), frågan hur man skall kunna åstadkomma snabbare beslut i fråga om hemliga tvångsmedel på teleområdet (avsnitt 11.4), frågan hur man snabbt skall kunna säkra annan elektronisk bevisning som riskerar att gå förlorad (avsnitt 11.5), behovet av anpassningar av befintliga tvångsmedel med hänsyn till den nya tekniken (avsnitt 11.6) samt frågan om den nuvarande begränsningen av tillämpningsområdet för hemliga tvångsmedel till telenät av mindre betydelse från kommunikationssynpunkt står i överensstämmelse med konventionen (avsnitt 11.7).

11.3 Tillämpningsområdena för hemlig teleavlyssning och hemlig teleövervakning

11.3.1 Ändrad gränsdragning mellan hemlig teleavlyssning och hemlig teleövervakning?

Förslag: Den nuvarande gränsen mellan hemlig teleavlyssning och hemlig teleövervakning bör behållas. Någon generell utvidgning av tillämpningsområdet för hemlig teleövervakning bör inte komma i fråga. Inte heller bör definitionen av vad som är ett telemeddelande ändras. Däremot bör definitionen flyttas från lagen om elektronisk kommunikation till rättegångsbalken.

Vid förebyggande, förhindrande och utredning av IT-relaterad brottslighet (och andra brott där datorer har spelat en viktig roll) är det framför allt tillgång till uppgifter om de elektroniska kommunikationsvägarna och de slutsatser som kan dras av dessa uppgifter som är av vital betydelse. Det kanske viktigaste i sammanhanget är trafikuppgifter. Med trafikuppgifter avses, som tidigare har nämnts, uppgifter om ett meddelandes ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av tjänst (t.ex. elektronisk post). Även lokaliseringsuppgifter kan i vissa fall ha betydelse. Med lokaliseringsuppgifter avses uppgifter om den geografiska positionen för den terminalutrustning som en användare utnyttjar sig av. Lokaliseringsuppgifter ger framför allt besked om var en mobiltelefonanvändare befinner sig. Sådana uppgifter torde generellt ha väsentligt större betydelse för utredning av andra typer av brott än IT-relaterade sådana, exempelvis grova narkotikabrott och annan organiserad brottslighet.

Både trafikuppgifter och sådana lokaliseringsuppgifter som avslöjar var den som kommunicerar befinner sig omfattas av reglerna om hemlig teleövervakning.

De nyligen införda utvidgningarna av tillämpningsområdena för hemlig teleavlyssning och hemlig teleövervakning innebär ett stort steg i riktning mot att Sverige uppfyller kraven i konventionen. Utvidgningarna är emellertid inte tillräckliga för att samtliga krav skall uppfyllas. För det första måste, om kravet på tillräckligt straffminimum för vissa brott inte är uppfyllt, det övervägas antingen om hemlig teleövervakning trots detta skall få användas, eller om någon annan lösning bör väljas som gör det möjligt att avslöja trafikuppgifter och lokaliseringsuppgifter. För det andra måste övervägas huruvida kravet på skälig misstanke utgör ett problem.

En generell lösning kan vara att utvidga tillämpningsområdet för hemlig teleövervakning, utöver vad regeringen har föreslagit i prop. 2002/03:74. En annan möjlighet är att ändra definitionen av vad som är ett telemeddelande, för att därigenom justera tillämpningsområdet för de hemliga tvångsmedlen.

En allmän utvidgning av tillämpningsområdet för hemlig teleövervakning, genom att tillåta användning av tvångsmedlet vid lindrigare brott än nu, är skenbart det enklaste sättet att lösa uppgiften att skapa ökad tillgång till uppgifter om datorkommunikation och bevisning i elektronisk form hos operatörer. Detta kan åstadkommas genom att man sänker kravet på att brotten skall ha lägst sex månaders fängelse i straffskalan. En sådan utvidgning är emellertid inte problemfri. Reglerna om hemliga tvångsmedel har nyligen varit föremål för en grundlig översyn. Regeringen föreslog, med Buggningsutredningens betänkande som grund, en betydande utvidgning av tillämpningsområdet för såväl hemlig teleavlyssning som hemlig teleövervakning. I vissa hänseenden gick regeringens förslag längre än utredningens. Mot bakgrund av att det är fråga om särskilt integritetskränkande tvångsmedel och att en total översyn har gjorts så nyligen ter det sig inte lämpligt att, innan dessa förslag har hunnit tillämpas i någon utsträckning, föreslå ytterligare en generell utvidgning.

En annan möjlighet skulle kunna vara att dra en ny gräns mellan hemlig teleavlyssning och hemlig teleövervakning. Man skulle t.ex., i stället för att använda begreppet telemeddelande för båda tvångsmedlen, kunna låta hemlig teleavlyssning ha samma tillämpningsområde som när tvångsmedlet ursprungligen tillskapades. Hemlig teleavlyssning tillkom för att ge brottsbekämpande myndigheter möjlighet att snappa upp innehållet i muntlig kommunikation via telefon, medan hemlig teleövervakning syftade till att försvåra sådan kommunikation genom att samtal förhindrades eller fördröjdes. I dag är det utan betydelse om kommunikationen är muntlig eller skriftlig. Begreppet telemeddelande täcker båda slagen av kommunikation. Eftersom det är spårandet av datorkommunikation som är det intressanta för anpassningen till konventionen skulle en ändrad gränsdragning mellan hemlig teleavlyssning och hemlig teleövervakning, som gör det möjligt att få del av innehållet i ett icke muntligt meddelande genom teleövervakning, kunna vara en lösning. Genom att det ställs väsentligt lägre krav på brottets svårhetsgrad vid hemlig

teleövervakning skulle de brottsbekämpande myndigheterna därigenom få tillgång till fler uppgifter än i dag.

Att använda samma tekniska avgränsning – begreppet telemeddelande – har emellertid stora praktiska fördelar, inte minst därför att båda tvångsmedlen mycket ofta förekommer i samma ärende (skr. 2003/04:36 s. 8). Uttrycket är dessutom teknikneutralt, vilket är något som också eftersträvas i konventionen.

Vidare är det en följd av den ökade integrationen mellan olika tekniska system som kan användas för elektronisk överföring av ljud, text och bilder att det är tekniskt och praktiskt svårt – och i vissa fall omöjligt – att skilja ut en viss typ av elektroniskt meddelande från en annan utan att först ta del av innehållet i telemeddelandet. Det skulle därför krävas ett större integritetsintrång för att sålla ut uppgifter hänförliga till hemlig teleövervakning, om man väljer den nu skisserade lösningen. Det bör inte heller vara avsändarens val av teknik som styr vilket straffprocessuellt tvångsmedel som kan användas. Starka sakliga skäl talar därför för att behålla den nuvarande avgränsningen mellan tvångsmedlen och för att behålla definitionen av vad som är ett telemeddelande.

En närliggande fråga är om denna definition bör flyttas från lagen om elektronisk kommunikation till rättegångsbalken. I propositionen med förslag till lag om elektronisk kommunikation framhöll regeringen att definitionen inte längre behövs för den lagstiftningen, men att den har betydelse bl.a. för regler i brottsbalken och rättegångsbalken. Därför behölls tills vidare definitionen i lagen om elektronisk kommunikation, i avvaktan på ytterligare översyn av de hemliga tvångsmedlen i rättegångsbalken (prop. 2002/03:110 s. 269). Frågan om definitionen och dess placering behandlades inte i propositionen om hemliga tvångsmedel.

På sikt framstår det som mindre lämpligt att definitionen av vad som är ett telemeddelande finns i en lagstiftning där den inte längre sakligt hör hemma. Definitionen har betydelse framför allt för reglerna om hemliga tvångsmedel i 27 kap. RB.[37] Det

[37] Begreppet telemeddelande används numera även i 4 kap. 8 § BrB.

finns därför goda skäl att flytta bestämmelsen dit, även om balken normalt inte har definitioner av detta slag. Några ändringar i definitionen bör inte göras.

Frågan är om man samtidigt bör byta ut begreppet telemeddelande mot det nya begrepp som används i lagen om elektronisk kommunikation, nämligen elektroniskt meddelande. Regeringen har nyligen gett tilläggsdirektiv till Beredningen för rättsväsendets utveckling. Enligt dessa direktiv (Dir. 2003:145 s. 7) skall beredningen se över det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. I uppdraget ingår bl.a. en anpassning och modernisering av rättegångsbalkens terminologi. Mot den bakgrunden tas inte frågan om begreppet telemeddelande bör bytas ut upp i detta sammanhang.

11.3.2 Skall en straffvärdeventil införas för hemlig teleövervakning?

Bedömning: Någon straffvärdeventil bör inte införas för hemlig teleövervakning. Inte heller i övrigt bör det göras några ändringar i de grundläggande förutsättningarna för att använda hemlig teleövervakning.

I föregående avsnitt har tanken på en ny gränsdragning mellan hemlig teleavlyssning och hemlig teleövervakning och på en generell utvidgning av tillämpningsområdet för hemlig teleövervakning till lindrigare brott avvisats. Om man vill utvidga tillämpningsområdet till att omfatta fler typer av brott finns det även andra lösningar som är tänkbara. En möjlighet är att för hemlig teleövervakning införa en straffvärdeventil av samma slag som nyligen har beslutats i fråga om hemlig teleavlyssning. Med straffvärdeventil avses en möjlighet att ta hänsyn till straffvärdet i det enskilda fallet. Eftersom straffskalorna ofta är mycket vida kan ett brott ha ett straffvärde som klart överstiger sex månaders fängelse men ändå ligga utanför tvångsmedlets tillämpningsområde eftersom minimistraffet inte uppgår till sex månaders fäng-

else. En annan möjlighet att utvidga tillämpningsområdet för hemlig teleövervakning är att föra in nya brott i uppräkningen av brott vid vilka det, trots att straffskalan inte når upp till den föreskrivna miniminivån, får förekomma hemlig teleövervakning.

Regeringen har inte varit främmande för att införa en straffvärdeventil även för hemlig teleövervakning. I lagrådsremissen om hemliga tvångsmedel fanns ett sådant förslag. I propositionen avstod emellertid regeringen från detta förslag, sedan lagrådet hade påpekat att konsekvensen skulle bli att hemliga tvångsmedel skulle kunna användas vid utredning av många brott som kan förväntas leda till en icke frihetsberövande påföljd. Regeringen valde i stället att utvidga den brottskatalog som anger för vilka brott hemlig teleövervakning får användas, trots att brotten inte har straffminimum om sex månaders fängelse (prop. 2002/03:74 s. 35). Frågan är om anpassningen till konventionen leder till en annan bedömning av behovet av en straffvärdeventil.

De skäl som regeringen nyligen anförde mot att införa en straffvärdeventil för hemlig teleövervakning har alltjämt samma bärkraft. Att enbart som ett led i anpassningen till konventionen ta ett avgörande steg i riktning mot en väsentlig utvidgning av tillämpningsområdet för hemlig teleövervakning bör inte komma i fråga, särskilt som en ny översyn har aviserats. Dessutom kan det vara av värde att ta del av erfarenheterna av en straffvärdeventil vid hemlig teleavlyssning, innan man går vidare med samma lösning för andra tvångsmedel.

En annan tänkbar lösning är att utvidga den katalog av brott vid vilka hemlig teleövervakning får användas trots att straffskalorna för brotten inte når upp till den miniminivå som annars krävs. Katalogen bör endast innehålla brott som ofta begås genom telemeddelanden och där det därför typiskt sett finns ett stort behov av att kunna använda tvångsmedlet (jfr prop. 2002/03:74 s. 35).

Beträffande brott enligt artiklarna 2-11 ställer konventionen krav på att staterna skall ha regler som gör det möjligt att snabbt få fram trafik- och lokaliseringsdata. Beträffande andra brott

som begås med hjälp av datorsystem kan förbehåll göras för krav enligt nationell lagstiftning.

Sedan brottskatalogen i 27 kap. 19 § RB utvidgades med brotten dataintrång och barnpornografibrott kan hemlig teleövervakning beslutas för brotten som motsvarar artiklarna 2-6 samt 9. I fråga om brotten i artiklarna 7 och 8 innebär strafftröskeln för hemlig teleövervakning att detta tvångsmedel kan användas vid grova brott. Det är således enbart i fråga om brott enligt artikel 10 (dvs. upphovsrättsintrång) som man över huvud taget inte har möjlighet att använda detta tvångsmedel.

Straffskalornas utformning vid brott mot upphovsrätt är av avgörande betydelse för frågan om det krävs några lagstiftningsåtgärder. Eftersom en översyn av sanktionssystemet för upphovsrättsintrång har aviserats (se avsnitt 6.6.3) bör utfallet av den avvaktas innan man tar slutlig ställning till genomförandet av konventionen i denna del. Först då finns det nämligen ett tillräckligt underlag för att bedöma behovet av ändringar och hur de i så fall bör utformas. Av nu nämnda skäl läggs därför inte något förslag i frågan fram i detta sammanhang.

Av det sagda följer att några ändringar i de grundläggande förutsättningarna för att använda hemlig teleövervakning inte bör göras.

11.3.3 Skälig misstanke

Förslag: Kravet på skälig misstanke för beslut om hemlig teleövervakning behålls. För att tillgodose kraven i konventionen på snabb tillgång till trafikuppgifter väljs i stället en annan lösning, som innebär att uppgiftsskyldigheten i lagen om elektronisk kommunikation utökas.

Ett grundläggande krav för beslut om hemlig teleövervakning är att det finns någon som är skäligen misstänkt. Regleringen i konventionen lägger inte fast några krav av det slaget utan utgår tvärtom från att trafikuppgifter och lokaliseringsuppgifter generellt skall vara åtkomliga vid utredning om brott. Samtidigt

framhålls, genom hänvisning till artiklarna 14 och 15, behovet av rättssäkerhetsgarantier.

Vid pågående dataintrång kan man ibland med relativt stor säkerhet utgå från att den dator som används som ett mellanled för angreppet tillhör en person eller ett företag som är ovetande om intrånget. I de fallen fokuseras intresset på att få fram uppgifter om kommunikationen, i syfte att spåra angreppet bakåt till den verklige gärningsmannen, vilken i många fall befinner sig i ett helt annat land.

Naturligtvis kan det anföras skäl för att en dator som används för att genomföra ett brott också leder till att den som förfogar över datorn kan misstänkas för delaktighet i brottet. Det kan förhålla sig så, men i många fall torde misstanken inte vara särskilt stark. En dator på en arbetsplats kan vara tillgänglig för flera personer och en dator i ett normalt hushåll är som regel åtkomlig för alla familjemedlemmar. Härutöver kan det i båda fallen finnas en större eller mindre krets av besökare som tillfälligt har kunnat utnyttja datorn. Vidare finns det datorer som är avsedda att användas av många, t.ex. datorer på bibliotek eller i skolor. Dessutom kan hackers utnyttja andras datorer genom att med tekniska åtgärder tillfälligt ta över kommandot över datorn. Vidare är det känt att s.k. IP-adresser – som är den teleadress som används vid kommunikation via Internet – kan missbrukas. Detta innebär att det ingalunda är självklart att den som äger eller brukar en dator alltid kan misstänkas för inblandning i ett brott där datorn har använts som hjälpmedel. Än mindre kan hävdas att misstanken regelmässigt når upp till nivån skälig misstanke.

Kravet på skälig misstanke för hemlig teleövervakning innebär att Sverige inte med nuvarande lagstiftning uppfyller åtagandena i konventionens artiklar 17 och 20 att snabbt få fram trafikuppgifter. Sådana uppgifter har framför allt betydelse för möjligheten att spåra upp en gärningsman, dvs. i situationer där det inte finns någon utpekad misstänkt. Det är därför nödvändigt att finna en lösning för hur kraven på snabbt säkrande och röjande av trafikuppgifter skall uppnås. Eftersom det är fråga om särskilt integritetskänsliga uppgifter bör denna lösning dels begränsas till

vad som krävs för att uppfylla åtagandena i konventionen, dels uppfylla höga krav på rättssäkerhet.

I den lagrådsremiss angående hemliga tvångsmedel som regeringen den 6 april 2000 överlämnade till lagrådet föreslogs att beslut om hemlig teleövervakning i vissa fall skulle kunna meddelas, trots frånvaro av någon skäligen misstänkt (s. 78). Förslaget skall ses mot bakgrund av att regeringen samtidigt föreslog att reglerna i telelagen om operatörers skyldighet att, utan hinder av tystnadsplikten, lämna uppgifter till bland annat polis och åklagare skulle ändras. Enligt förslaget skulle inhämtande av uppgifter angående särskilda telemeddelanden regleras enbart i rättegångsbalken. I den proposition som senare överlämnades till riksdagen fanns de nu redovisade förslagen inte med.

Genomförandet av konventionen aktualiserar på nytt problemet med två parallella system med regler om utlämnande av uppgifter om telemeddelanden, särskilt som dessa skiljer sig kraftigt i fråga om tre grundläggande moment, nämligen

- vem som beslutar om utlämnande,
- kraven på brottets svårhet och betydelsen av uppgifterna för utredningen samt
- kraven på brottsmisstanke.

I lagen om elektronisk kommunikation ställs betydligt lägre formella krav för röjande av uppgifter än vad som gäller för hemlig teleövervakning. Enligt lagen om elektronisk kommunikation kan vilken polisman, tulltjänsteman eller åklagare som helst få ut uppgifter om telemeddelanden, medan det för hemlig teleövervakning krävs att en domstol bifaller åklagarens framställning om hemlig teleövervakning. I lagen om elektronisk kommunikation ställs däremot högre krav på brottets svårhetsgrad (lägst två års fängelse i straffskalan) än för hemlig teleövervakning (lägst sex månaders fängelse). I gengäld kräver lagen om elektronisk kommunikation inte misstanke mot någon utpekad person, medan det för hemlig teleövervakning krävs dels skälig misstanke dels viss anknytning mellan den misstänkte och teleadressen. Det innebär t.ex. att uppgifter om telemeddelanden till och från målsägande och vittnen är åtkomliga enligt lagen om elektronisk

kommunikation men inte enligt rättegångsbalken. Medan lagen om elektronisk kommunikation inte uppställer några krav på att det skall vara av betydelse för utredningen att uppgifterna lämnas, ställs det för hemlig teleövervakning krav på att uppgifterna skall vara av synnerlig vikt för utredningen.

I avvaktan på den utredning som har aviserats (Dir. 2003:145) läggs inte här fram något förslag om att reglera utlämnande av uppgifter om telemeddelanden uteslutande i den ena eller andra lagstiftningen, även om en enhetlig lösning skulle ha underlättat anpassningen till konventionen.

Det som krävs för att uppfylla åtagandena i konventionen är en möjlighet att få fram trafikuppgifter, däribland även lokaliseringsuppgifter. Tillämpningsområdet för en ny regel bör därför begränsas till sådana uppgifter. Vidare skall det vara fråga om uppgifter som hänför sig till en särskilt utpekad kommunikation. Med andra ord bör regeln inte ha samma vida tillämpningsområde som bestämmelsen om hemlig teleövervakning, som bl.a. medger en kontroll av all kommunikation till och från en teleadress under en viss angiven tidsperiod.

En regel som i större utsträckning än nu medger tillgång till trafikuppgifter kan placeras antingen i rättegångsbalken eller i lagen om elektronisk kommunikation.

För en placering i rättegångsbalken talar att det är fråga om en processuell åtgärd som hör hemma i en förundersökning. Vidare innebär en sådan lösning att reglerna om tvångsåtgärder på teleområdet i största möjliga utsträckning hålls samlade och att de rättssäkerhetsgarantier som ligger i att besluten prövas av domstol automatiskt kommer att gälla. Att det har förts en diskussion om att reglerna om uppgiftslämnande i lagen om elektronisk kommunikation av rättssäkerhetsskäl skall föras samman med reglerna i rättsgångsbalken talar också för denna lösning. I samma riktning talar det förhållandet att det finns en parlamentarisk kontroll av användningen av hemliga tvångsmedel, men inte någon särskild kontroll av hur reglerna om utlämnande i lagen om elektronisk kommunikation tillämpas. Vad som främst talar emot placeringen i rättegångsbalken är att man antingen

måste överge kravet på skälig misstanke för ett av de mest integritetskänsliga tvångsmedlen eller tillskapa ett nytt tvångsmedel utan krav på brottsmisstanke. Europadomstolens krav på tydliga lagregler och en utpekad krets av personer som kan drabbas av hemliga tvångsmedel på teleområdet, för att regleringen inte skall stå i strid med Europakonventionens artikel 8, gör en sådan lösning diskutabel.

För en lösning som bygger vidare på reglerna i lagen om elektronisk kommunikation talar först och främst att reglerna om uppgiftslämnande i 6 kap. 22 § inte kräver brottsmisstanke mot viss person. Det som behövs för att uppfylla kraven i konventionen är att enstaka uppgifter av begränsad natur om ett visst eller vissa kommunikationstillfällen kan lämnas ut, medan hemlig teleövervakning som nyss nämnts har ett generellt användningsområde. Det är också lagtekniskt enkelt att bygga ut nuvarande bestämmelser i 6 kap. 22 § med ytterligare någon punkt, även om den paragrafen redan är mycket omfattande. Det som främst talar emot en placering i lagen om elektronisk kommunikation är att prövningen av om uppgifter skall lämnas ut sker på ett mindre rättssäkert sätt (se JO 1997/98 s. 47 ff och SOU 1998:46 s. 371 ff). I artikel 17 framhålls nämligen kravet på betryggande rättssäkerhetsgarantier.

Vid en sammanvägning av skälen för och emot att utvidga tillämpningsområdet för hemlig teleövervakning talar ändå, i avvaktan på en samlad bedömning av hur regelsystemet skall vara utformat, övervägande skäl för att det är lämpligare att placera en regel om röjande av trafikuppgifter rörande enstaka kommunikationstillfällen i lagen om elektronisk kommunikation. Frågan behandlas därför vidare i avsnitt 11.8.3.

11.4 Ett nytt tvångsmedel

11.4.1 Vad innebär frysning av elektronisk kommunikation?

Förslag: Ett nytt tvångsmedel, frysning av elektronisk kommunikation, införs. Ändamålet med tvångsmedlet skall 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 innebär att uppgifter om elektronisk kommunikation efter särskilt beslut tillfälligt skall bevaras av operatören i avvaktan på att domstol tar ställning till om hemlig teleavlyssning eller hemlig teleövervakning skall tillåtas. Först när ett domstolsbeslut om tvångsmedel har meddelats får uppgifterna lämnas ut. Bestämmelser om frysning av elektronisk kommunikation tas in i 27 kap. RB.

Förutsättningarna för ett nytt tvångsmedel

Enligt artikel 20 skall parterna ha en lagstiftning som gör det möjligt att i realtid samla in trafikuppgifter som hänför sig till särskilt angivna elektroniska meddelanden. I artikel 21 ställs det krav på lagstiftning som gör det möjligt att i realtid samla in uppgifter om innehållet i sådana meddelanden. Enligt artikel 16 skall det vara möjligt att snabbt säkra lagrade datauppgifter och enligt artikel 17 skall trafikuppgifter som har säkrats med stöd av artikel 16 snabbt kunna röjas för behöriga myndigheter. Dessa åtaganden innebär att det måste skapas regler som gör det möjligt att snabbare än nu säkra och få ut uppgifter om elektronisk kommunikation.

Uppgifter om elektronisk kommunikation kringgärdas med sekretess hos operatören och får dessutom normalt inte sparas. En grundläggande förutsättning för att uppgifter om elektronisk kommunikation hos en operatör skall kunna säkras som bevisning är givetvis att uppgifterna antingen är lagrade eller att det är fråga om uppgifter som kan hämtas in i framtiden.

En operatör skall enligt huvudregeln utplåna eller avidentifiera trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter när uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande (6 kap. 5 § lagen om elektronisk kommunikation). Med trafikuppgifter avses i den be-

stämmelsen, enligt 6 kap. 1 §, uppgifter som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande.

Det bör införas ett helt nytt tvångsmedel som tillgodoser kraven i konventionen på skyndsamt säkrande av uppgifter som rör elektronisk kommunikation i realtid, men som samtidigt uppfyller integritetskraven i direktivet om integritetsskydd och elektronisk kommunikation (2002/58/EG; i fortsättningen benämnt teledataskyddsdirektivet). Tvångsmedlet skall öka möjligheterna att bevara spåren av elektronisk kommunikation. Sådana spår kan snabbt försvinna på grund av skyldigheten för operatörer att utplåna eller avidentifiera trafikuppgifter så snart de inte längre behövs. Det är således mycket angeläget att det, genom ett snabbt ingripande av brottsbekämpande myndigheter, kan förhindras att viktig information utplånas.

Enligt teledataskyddsdirektivets artikel 15.1 får medlemsstaterna besluta om begränsningar i fråga om bl.a. trafikuppgifter och sekretess till skydd för abonnenten när en sådan begränsning är nödvändig, lämplig och proportionell i syfte bl.a. att förebygga, uppdaga, utreda och åtala brott eller vid obehörig användning av ett elektroniskt kommunikationssystem. För sådant ändamål får medlemsstaterna besluta om lagstiftning som innebär att uppgifter bevaras under en begränsad period som motiveras av nyss angivna skäl. Ett nytt tvångsmedel är således väl förenligt med åtagandena i direktivet.

Benämningen på det nya tvångsmedlet

En viktig fråga är hur det nya tvångsmedlet bör benämnas. Man bör undvika en benämning som ger intryck av att det är fråga om interimistiska beslut om hemliga tvångsmedel på teleområdet. Tvångsmedlet bör därför, i likhet med förvar och anhållande, ha en egen benämning. I konventionen talas det om säkrande. Man skulle därför kunna kalla det nya tvångsmedlet ”snabbsäk-

rande".[38] En sådan benämning är dock intetsägande eftersom de flesta tvångsmedel har till syfte att snabbt säkra bevisning, ekonomiska tillgångar eller den misstänktes person. En annan möjlighet är att kalla det "kommunikationsspärr". Det namnet för dock tankarna mera till en teknisk än en juridisk åtgärd. Inget av de nu nämnda förslagen är således lyckat. Man bör i stället välja en term som dels är särskiljande, dels språkligt ger en känsla av vad det är fråga om för tvångsmedel. Det är också en fördel om den knyter an till befintlig terminologi.

Som tidigare har nämnts (avsnitt 6.12.3) pågår för närvarande arbete med att anpassa den svenska lagstiftningen till rambeslutet om verkställighet av beslut om frysning av egendom eller bevismaterial. Termen frysning används i rambeslutet som ett samlande begrepp för olika åtgärder som innebär att tillgångar eller bevismaterial snabbt säkras för att förhindra att de går förlorade. Förfarandet att snabbt säkra spåren av elektronisk kommunikation har i grunden samma syfte. Därför har det nya tvångsmedlet benämnts frysning av elektronisk kommunikation.

Ändamålet med tvångsmedlet

Frysning av elektronisk kommunikation skall utgöra ett kort förstadium till domstols beslut om hemlig teleavlyssning eller hemlig teleövervakning. Bestämmelsen om frysning bör således knytas till de nuvarande reglerna om dessa tvångsmedel. Med den lösningen kommer frysning att omfatta alla typer av telemeddelanden, dvs. såväl ljud, text, bild, data som information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare. Den nya bestämmelsen har sin naturliga plats i 27 kap. RB.

Ändamålet med frysning skall vara att, i avvaktan på att domstol tar ställning till användningen av hemliga tvångsmedel på området för elektronisk kommunikation, förhindra att bl.a. tra-

[38] I Danmark har institutet benämningen "hastesikring".

fikuppgifter och andra uppgifter om kommunikationen går förlorade. Även om en jourdomstol kan besluta om hemliga tvångsmedel är det inte självklart att ett sådant beslut kan utverkas med den snabbhet som kan vara nödvändig för att kunna spåra elektronisk kommunikation innan den utplånas. Vid ett pågående dataintrång kan det krävas beslut omedelbart, vilket innebär att det inte finns tid att göra en formell framställning till domstol. Beslut om frysning bör därför fattas av någon annan myndighet än domstol. Frågan om vem som skall besluta om frysning behandlas i avsnitt 11.4.3.

Med den föreslagna lösningen innebär frysning enbart ett beslut om att viss bevisning tillfälligt skall bevaras till dess domstol har tagit ställning till frågan om användning av hemliga tvångsmedel. Införandet av frysning har inte till syfte att förändra en operatörs skyldighet att *lämna ut uppgifter* om elektronisk kommunikation. Skyldigheten att lämna uppgifter till de brottsbekämpande myndigheterna bör, om det inte följer av någon annan regel att uppgiften skall lämnas, inträda först när det finns ett domstolsbeslut om hemlig teleavlyssning eller hemlig teleövervakning. Med den lösningen kommer inget integritetsintrång att äga rum om domstolen skulle avslå framställningen om att använda hemliga tvångsmedel, samtidigt som man tillgodoser behovet av ett snabbt beslut som förhindrar radering av uppgifterna. Den nu föreslagna lösningen innebär däremot att operatörernas skyldighet att *tillfälligt bevara uppgifter* påverkas. Dessa blir skyldiga att bevara de uppgifter som omfattas av ett beslut om frysning till dess att en domstol har hunnit ta ställning i frågan om användning av hemliga tvångsmedel, vilket föreslås ske inom loppet av några dagar.

Vid utformningen av förslaget om frysning har beaktats de begränsningar som följer av artikel 15 i teledataskyddsdirektivet. Den lösning som har valts står i god överensstämmelse med bestämmelserna i direktivet. Den kommer inte heller i konflikt med bestämmelserna i artikel 6 och artikel 8 i Europakonventionen, eftersom den bygger på befintliga tvångsmedel som uppfyller konventionens krav.

11.4.2 Förutsättningarna för frysning av elektronisk kommunikation

Förslag: Samma förutsättningar skall gälla för frysning av elektronisk kommunikation som för beslut om hemlig teleavlyssning eller hemlig teleövervakning.

Med den lagtekniska lösning som har valts uppkommer frågan vilka krav som bör ställas för beslut om frysning av elektronisk kommunikation.

De nuvarande tvångsmedelsreglerna erbjuder två alternativa modeller. Den ena modellen är att låta exakt samma krav gälla för ett tvångsmedel som är temporärt i avvaktan på domstolsprövning. Förvar och kvarstad utgör exempel på detta. Den andra modellen är att det i något avseende ställs lägre krav för beslut om det temporära tvångsmedlet. Som exempel på detta kan nämnas att det för utredningsanhållande ställs lägre krav än för utredningshäktning i fråga om vilka utredningsåtgärder som skall vidtas. Däremot är kraven desamma i fråga om bl.a. brottets svårhetsgrad och graden av misstanke.

Med tanke på att de hemliga tvångsmedlen anses särskilt integritetskänsliga bör man välja den förstnämnda modellen, dvs. att ställa samma krav för frysning av elektronisk kommunikation som för hemlig teleavlyssning respektive hemlig teleövervakning.

Det innebär för det första att det krävs skälig misstanke om brott av sådan svårhetsgrad eller av sådant slag att hemlig teleavlyssning respektive hemlig teleövervakning kan beslutas. Dessutom krävs det att åtgärden är av synnerlig vikt för utredningen, vilket i princip innebär att alla andra utredningsmöjligheter skall vara uttömda eller inte möjliga att använda i det enskilda fallet (prop. 1988/89:124 s. 44). Härutöver skall den teleadress som berörs av åtgärden ha viss nära anknytning till den misstänkte.

Den som beslutar om frysning måste således göra samma bedömning som domstolen gör i fråga om användningen av hemliga tvångsmedel på teleområdet. Det innebär också att de generella begränsningar som gäller för hemlig teleavlyssning, t.ex. att samtal eller andra telemeddelanden som utväxlas mellan den

misstänkte och hans försvarare inte får avlyssnas, gäller även för frysning. Vad som har sagts om tillämpningen av proportionalitetsprincipen vid användning av hemliga tvångsmedel (prop. 1988/89:124 s. 66) skall självfallet tillämpas vid beslut om frysning.

11.4.3 Vem skall besluta om frysning av elektronisk kommunikation?

Förslag: Beslut om frysning av elektronisk kommunikation skall meddelas av åklagare. Frysningsbeslutet skall underställas domstol så snart som möjligt och senast andra dagen efter beslutet. Åklagaren skall inom den angivna tiden ge in en framställning om hemlig teleavlyssning eller hemlig teleövervakning. Om ingen framställning görs skall åklagaren omedelbart häva beslutet. Åklagaren skall underrätta operatören om beslut att häva frysning.

Beslut av åklagare

För att en regel om frysning av elektronisk kommunikation skall få någon praktisk betydelse måste ett beslut kunna fattas mycket snabbt. Detta gäller särskilt i de fall en viss kommunikation behöver spåras i realtid.

Frysning utgör ett interimistiskt förstadium till domstolens ställningstagande i frågan om hemliga tvångsmedel. Den föreslagna konstruktionen, där frågan om frysning snabbt skall föras under domstolsprövning, innebär att beslutanderätten måste ligga på någon som dels uppfyller kraven på kvalificerad juridisk kompetens, dels för talan inför domstol i brottmål. En förutsättning för den föreslagna konstruktionen är vidare att det finns ett system med jour eller beredskap för att tillgodose behovet av snabba beslut även utanför kontorstid. De enda som uppfyller de nu angivna kraven är åklagare. Det är därför naturligt att låta åklagare fatta beslut om frysning, på samma sätt som åklagare

fattar beslut i fråga om anhållande som förstadium till häktning eller förvar som förstadium till kvarstad.

Man kan naturligtvis ställa sig frågan om man, i stället för att införa regler om frysning, bör ge åklagare rätt att fatta interimistiska beslut om hemlig teleavlyssning och hemlig teleövervakning. Regeringen har nyligen tagit ställning till den frågan i samband med utvidgningen av reglerna om hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken (prop. 2002/03:74). Regeringen fann att det för närvarande inte bör införas någon ytterligare möjlighet för åklagare att fatta interimistiska beslut i fråga om hemliga tvångsmedel, men förklarade sig ha för avsikt att noga följa utvecklingen och vid behov pröva frågan på nytt (a. prop. s. 42 f). Något principiellt hinder mot att låta åklagare besluta interimistiskt om sådana tvångsmedel torde därför inte finnas. Å andra sidan har åklagarens möjlighet att interimistiskt besluta om hemlig teleavlyssning enligt 1952 års lag ytterst sällan utnyttjats. Det finns därför ingen erfarenhet av sådana beslut inom åklagarkåren. Operatörerna har på grund av detta inte någon vana vid att hantera åklagarbeslut. Ett beslut om frysning innebär inte någon egentlig integritetskränkning, medan ett interimistiskt beslut om hemliga tvångsmedel skulle ha samma verkan som ett beslut av domstol, nämligen att operatörerna omedelbart skall lämna ut den säkrade informationen. Vad som nu har sagts, i förening med att regeringen nyligen har tagit ställning mot att låta åklagare få utökad beslutanderätt i fråga om hemliga tvångsmedel, talar för att man bör välja lösningen med frysning framför att ge åklagare en interimistisk beslutanderätt.

En annan fråga är om man bör begränsa kretsen beslutsfattare bland åklagarna. Vad som kan tala för en sådan lösning är att frysning av elektronisk kommunikation är en åtgärd som åklagaren snabbt måste ta ställning till, att beslut om frysning ställer stora krav på den juridiska kompetensen, att det med kort varsel kan krävas direktkontakt med ett annat lands myndigheter (vilket bl.a. förutsätter goda språkkunskaper) samt att det kan krävas god kännedom om hur man handlägger framställningar om internationell rättslig hjälp. Det sagda talar för att bara åklagare

med viss kompetens bör få besluta. Å andra sidan kan en fråga om frysning aktualiseras var som helst i landet och när som helst. Det är viktigt att rättslig hjälp på begäran av en främmande stat inte fördröjs till följd av begränsningar i behörigheten. Att i lag eller annan författning begränsa vilka åklagare som får fatta beslut om frysning bör därför inte komma i fråga.

Om åklagare ges rätt att besluta om frysning av elektronisk kommunikation är det en naturlig uppgift för ledningen inom åklagarväsendet att noga följa utvecklingen och att vid behov lämna anvisningar eller utfärda föreskrifter för handläggningen. Då riksåklagaren har en generell rätt att utfärda föreskrifter för åklagarverksamheten kan denne, om det visar sig nödvändigt, genom föreskrifter reglera vilka åklagare som skall besluta om frysning av elektronisk kommunikation.[39]

Ett åklagarbeslut om frysning tillgodoser kraven på ett snabbt ingripande för att förhindra att viktig bevisning går förlorad. Ett sådant beslut bör emellertid, som nyss har sagts, inte ha någon annan verkan än att det gäller till dess domstol har hunnit ta ställning i frågan om det finns förutsättningar för att bevilja hemlig teleavlyssning eller hemlig teleövervakning. Ett frysningsbeslut bör därför så snabbt som möjligt underställas domstols prövning.

Frågan är hur stränga krav som skall ställas på en snabb underställning. Å ena sidan kan hävdas att det, när frysning har beslutats, inte är så bråttom med underställningen eftersom operatören då sparar uppgifter om den trafik som förekommer. Å andra sidan är det fråga om en mycket integritetskränkande åtgärd som, om den inte har tillräcklig grund, bör upphöra så snabbt som möjligt. En annan aspekt som bör vägas in är att domstolen måste få viss tid för att hinna sätta ut saken till sammanträde. Systemet med offentliga ombud innebär sannolikt att det inte går lika snabbt som tidigare att få till stånd sammanträden där frågor om hemliga tvångsmedel behandlas, eftersom det är en presumtion för att det offentliga ombudet skall närvara. Den

[39] Jfr föreskrifterna i Riksåklagarens författningssamling (RÅFS) 2002:5 om åklagares särskilda beredskapstjänstgöring för olagliga utsläpp från fartyg m.m. och RÅFS 2003:4 om särskild beredskap vid de internationella åklagarkamrarna.

komplikationen finns dock inte i ärenden om hemlig teleövervakning. Vidare måste beaktas att beslut om hemliga tvångsmedel normalt är förbehållna en liten krets av domare och att det är en typ av ärenden som det inte är lämpligt att jourdomstol avgör annat än i rena undantagsfall.

En lämplig avvägning kan vara att föreskriva att åklagaren så snart som möjligt och senast andra dagen efter frysningsbeslutet skall ansöka om hemlig teleavlyssning eller hemlig teleövervakning. Har en sådan ansökan getts in gäller frysningen till dess att domstolen har tagit ställning till åklagarens framställning.

Om åklagaren inte fullföljer frysningsbeslutet med att underställa domstolen frågan om tillstånd till hemlig teleavlyssning eller hemlig teleövervakning skall åklagaren omedelbart häva frysningsbeslutet. Det är angeläget att operatören så snabbt som möjligt underrättas om att frysningen har upphört, för att inte integritetskänsliga uppgifter skall bevaras i onödan. Åklagaren bör därför åläggas att underrätta operatören, om ett beslut om frysning hävs. Detta kan lämpligen ske genom att det införs en regel om underrättelse i förordningen (1964:740) med föreskrifter för åklagare i vissa brottmål. Underrättelseskyldigheten bör även omfatta de fall där rätten har avslagit åklagarens framställning om hemlig teleavlyssning eller hemlig teleövervakning. Att underrättelseskyldigheten läggs på åklagaren innebär självfallet inte något krav på att denne personligen måste underrätta operatören. Uppgiften kan delegeras, men ansvaret för att underrättelsen når fram vilar på åklagaren

Bör polisen få fatta interimistiska beslut?

Frågan är om en ordning med åklagarbeslut är tillräcklig för de allra mest brådskande fallen. I ett hypotetiskt fall kan brottsbekämpande myndigheter i ett annat land, som är ett allvarligt databrott på spåren, plötsligt upptäcka att kommunikationen tar vägen via en svensk dator och att det därför finns ett omedelbart behov av att säkra trafikuppgifter eller uppgifter om innehållet i ett telemeddelande, eftersom dessa annars riskerar att gå förlo-

rade. Det kan inte uteslutas att det i ett extremt fall kan krävas en så snabb kontakt med operatören för omedelbar säkring av uppgifterna att en kontakt med åklagare för beslut om frysning innebär en risk att bevisningen kan gå förlorad.

Det finns med andra ord skäl att överväga om man, för att göra regleringen heltäckande, bör ge polisen en möjlighet att vidta interimistiska åtgärder i avvaktan på åklagarens ställningstagande, på samma sätt som en polisman i brådskande fall kan besluta om gripande för att skapa praktiska förutsättningar för att åklagaren skall kunna besluta om anhållande.

Vad som kan tala för en sådan lösning är två omständigheter. Den ena är att ett beslut om frysning innebär att information skall bevaras, inte att informationen skall lämnas ut till de brottsbekämpande myndigheterna. Den andra är att polisen i dag har rätt att begära att få ut vissa uppgifter med stöd av lagen om elektronisk kommunikation.

Beslut om frysning kräver komplicerade juridiska ställningstaganden av samma slag som krävs för beslut om hemliga tvångsmedel. I motsats till åklagare, som under lång tid dels har ansvarat för ansökan hos domstol om hemliga tvångsmedel dels haft rätt att fatta beslut i sådana frågor enligt 5 § andra stycket 1952 års lag, har polisen ingen erfarenhet av de rättsliga bedömningar som krävs. Det är också fråga om de mest integritetskränkande tvångsmedlen i svensk rätt, där kraven på rättssäker handläggning är särskilt stora. Om det för utlämnande av informationen i princip krävs att domstol har beslutat om hemlig teleavlyssning eller hemlig teleövervakning kan det synas som om beslut om frysning inte har så stor betydelse att det skulle spela någon roll om man ger polisen rätt att besluta interimistiskt. Erfarenheterna visar emellertid att om en tvångsmedelsfråga har hanterats fel från början är risken betydande att felet inte upptäcks och att även den fortsatta handläggningen blir fel. Ett ingripande som saknat lagliga förutsättningar kan lätt leda till svåra konsekvenser för den enskilde som drabbats av beslutet. Det torde också bli fråga om få ärenden som är så extremt brådskande att en åklagarkontakt skulle innebära en riskabel fördröjning. Möjlighe-

terna för företrädare för polisen att skaffa rutin blir då mycket begränsade. Det kan därför aldrig bli tal om att ge beslutanderätt till en större grupp personer. Allt detta, i förening med att lagstiftaren har tvekat inför att anförtro åklagare beslutsfunktioner i fråga om hemliga tvångsmedel, talar med styrka emot att ge polisen rätt att fatta beslut i avvaktan på att åklagaren hinner kontaktas.

Polisens rätt att begära vissa uppgifter från operatörer kan inte heller ses som något starkt argument för att polisen skall ges möjlighet att besluta om interimistisk frysning, eftersom ordningen med utlämnande av information om telemeddelanden har ifrågasatts och förslag har lagts om avskaffande av denna rätt (SOU 1998:46 s. 367 ff). Frågan skall nu på utredas på nytt (Dir 2003:145).

Slutsatsen blir således att det inte bör införas någon möjlighet för polisen att ingripa interimistiskt innan åklagare har hunnit ta ställning till frågan om frysning.

Verkan av ett beslut om frysning av elektronisk kommunikation

Ett beslut om frysning av elektronisk kommunikation skall, i likhet med andra åklagarbeslut om tvångsmedel, gälla omedelbart.

Om domstolen beslutar om hemlig teleavlyssning eller hemlig teleövervakning upphör frysningsbeslutet automatiskt. Domstolens beslut leder till att den information som har samlats in med stöd av frysningsbeslutet blir åtkomlig, om tillståndet omfattar frysningstiden. Först genom domstolens beslut inträder således operatörens skyldighet att låta polis och åklagare få tillgång till innehållet i telemeddelandena respektive uppgifter om telemeddelandena eller lokaliseringsuppgifter som omfattas av beslutet.

Beslutar domstolen att avslå åklagarens framställning skall den omedelbart häva beslutet om frysning. Därmed upphör operatörens skyldighet att bevara det material som har samlats in med

anledning av frysningsbeslutet. Frågor om överklagande och inhibition tas upp i närmast följande avsnitt.

11.4.4 Handläggningen

Förslag: Ett beslut om frysning av elektronisk kommunikation skall innehålla samma uppgifter som ett beslut om hemlig teleavlyssning eller hemlig teleövervakning. En frist införs för domstolens handläggning. Om frysning av elektronisk kommunikation har beslutats skall domstolen hålla förhandling så snart det kan ske och senast på fjärde dagen efter det att framställningen kom in till domstolen. Befintliga regler om överklagande och inhibition är tillräckliga.

Åklagarnas handläggning

På ett beslut om frysning av elektronisk kommunikation bör ställas samma krav som på ett beslut om hemlig teleavlyssning och hemlig teleövervakning. I beslutet skall således anges om frysningen avser hemlig teleavlyssning eller hemlig teleövervakning (eller båda tvångsmedlen). Det innebär att beslutet skall vara skriftligt. Vidare behöver operatören samma uppgifter som finns i ett domstolsbeslut om hemliga tvångsmedel för att beslutet skall kunna verkställas, bl.a. uppgift om den eller de teleadresser som frysningen omfattar. Lagtekniskt bör detta lösas genom en hänvisning till motsvarande regler för domstolen (27 kap. 21 § RB). Därigenom kommer även kravet på att tiden för åtgärden inte får bestämmas längre än nödvändigt att gälla.

Ett åklagarbeslut om frysning torde i många fall kunna begränsas till det eller de telemeddelanden som avser ett visst kommunikationstillfälle, dvs. historiska uppgifter. Om beslutet skall avse frysning av framtida kommunikation till eller från en viss teleadress ligger det i sakens natur att tillståndet inte bör avse längre tid än fram till dess att domstol hinner ta ställning i frågan. Ett åklagarbeslut om frysning bör därför aldrig avse max-

imal tillståndstid för hemliga tvångsmedel på teleområdet, som är en månad.

Utformningen av frysningsbeslutet är viktig även från andra utgångspunkter. Eftersom besluten sannolikt oftast kommer att avse kommunikation i förfluten tid är det särskilt viktigt att omfattningen noggrant preciseras i beslutet.

Då det är en helt ny uppgift för åklagarväsendet att besluta om frysning av elektronisk kommunikation får det förutsättas att ledningen inom åklagarväsendet överväger utbildningsbehovet och under ett inledande skede noga följer utvecklingen samt vid behov utfärdar föreskrifter eller allmänna råd för åklagarnas handläggning.

Handläggningen i domstol

Handläggningen i domstol kommer i princip inte att vara annorlunda i ett ärende om hemlig teleavlyssning eller hemlig teleövervakning som initieras genom att åklagaren underställer rätten ett beslut om frysning än i andra ärenden om användning av sådana tvångsmedel.

När en framställning om tillstånd till ett hemligt tvångsmedel kommer in till domstolen finns det inte någon bestämd tidsfrist inom vilken frågan skall ha avgjorts. Det ligger emellertid i sakens natur att sådana ärenden skall handläggas så snabbt som möjligt. Numera är det obligatoriskt med sammanträde i ärenden om hemlig teleavlyssning (se 27 kap. 28 § RB). Ett offentligt ombud skall förordnas snarast och därefter skall ett sammanträde hållas, men någon formell frist för handläggningen har inte föreskrivits.

Saken kommer i ett annat läge om man inför åklagarbeslut om frysning av elektronisk kommunikation. Då finns det ett tvångsmedel som löper och vars fortsatta varaktighet domstolen bör ta ställning till snarast. Det bör därför anges en frist inom vilken domstolen skall pröva åklagarens beslut.

En sådan frist kan, om den görs alltför kort, komma att ställa ökade krav på tillgänglighet hos domstolarna och dessutom leda

till att beslut om hemliga tvångsmedel i större utsträckning än nu måste fattas av jourdomstol. Detta är något som om möjligt bör undvikas, med hänsyn till de hemliga tvångsmedlens särskilda karaktär. Fristen kan lämpligen bestämmas på samma sätt som för beslag, vilket innebär att domstolen skall hålla förhandling så snart det kan ske och senast på fjärde dagen efter det att framställningen kom in till domstolen. Med den lösningen torde det sällan vara nödvändigt att låta en jourdomstol ta ställning i ett frysningsärende. Samtidigt bör understrykas att domstolen endast i undantagsfall bör utnyttja hela fristen. Det ligger ju i sakens natur att ett ärende om användning av hemliga tvångsmedel som har initierats genom frysning är särskilt brådskande.

I domstolens beslut om hemlig teleavlyssning eller hemlig teleövervakning skall anges vilken tid tillståndet avser. Om frysning har föregått beslutet bör det av tillståndet framgå om det omfattar sådan information som varit föremål för frysning. Detta kommer att vara nödvändigt för att operatörerna skall kunna lämna ut uppgifterna (se avsnitt 11.10.1 angående ändringar i lagen om elektronisk kommunikation).

Eftersom frysning av elektronisk kommunikation enbart utgör ett förstadium till hemlig teleavlyssning respektive hemlig teleövervakning behövs det inte några särskilda regler om överklagande. Om domstolen avslår en framställning om hemlig teleavlyssning eller hemlig teleövervakning kan åklagaren överklaga det beslutet enligt 49 kap 5 § RB (punkt 6). Likaså kan, i ärenden om hemlig teleavlyssning, det offentliga ombudet överklaga ett beslut om användande av sådant tvångsmedel.

Vidare kan åklagaren, om han överklagar ett avslagsbeslut, begära inhibition avseende uppgifter som omfattats av ett beslut om frysning. Ett beslut om inhibition kan förhindra att uppgifterna raderas. Överinstansen kan besluta om inhibition utan att höra den misstänkte eftersom det är fråga om hemliga tvångsmedel (se prop. 2002/03:74 s. 31).

11.4.5 Verkställighetsfrågor

Bedömning: Det behövs inte några nya regler i rättegångsbalken för verkställigheten av frysning av elektronisk kommunikation. Däremot krävs det ändringar i lagen om elektronisk kommunikation.

Beslut om hemlig teleavlyssning eller hemlig teleövervakning verkställs av vederbörande operatör, som skall få del av domstolens beslut. Operatören får uppdraget via Säkerhetspolisen. Inom polisen är det nämligen Säkerhetspolisen som ansvarar för tekniska och administrativa frågor som rör dessa hemliga tvångsmedel.[40] Säkerhetspolisen sköter alla kontakter med operatörerna och förvaltar de tekniska system som används för att ta emot och bearbeta informationen från operatörerna. Varje polismyndighet har emellertid särskild personal som arbetar med systemet för hemlig teleavlyssning och hemlig teleövervakning. Den enhet vid Säkerhetspolisen som handhar hemliga tvångsmedel på teleområdet bedriver verksamhet dygnet runt hela året. Därmed finns det förutsättningar för att hantera brådskande fall.

Om åklagare ges rätt att besluta om frysning torde detta inte vålla några särskilda problem på verkställighetsstadiet i och med att förslaget bygger på redan befintliga tvångsmedel. Åklagarens beslut skall vidarebefordras till operatören på samma sätt som i dag är fallet med rättens beslut.

Det finns redan i dag möjlighet att med kort varsel verkställa ett beslut om hemlig teleavlyssning eller hemlig teleövervakning, om det finns behov av det. Kostnaderna för verkställighet utanför kontorstid kan dock vara en hämmande faktor (se SOU 2003:74 s. 252). Den frågan behandlas vidare i avsnitt 11.12.2.

Om frysningsbeslutet inte följs av ett domstolsbeslut om hemlig teleavlyssning eller hemlig teleövervakning kommer enbart operatören att ha tillgång till uppgifter om den kommunikation som har förekommit efter beslutet. Det krävs således vissa

[40] För en närmare beskrivning se Rikspolisstyrelsens föreskrifter RPSFS 1999:9 (FAP 171-1). Se även Ds 2003:13 s. 51.

följdändringar i lagen om elektronisk kommunikation medan det inte krävs några nya regler för polisens verksamhet (se avsnitt 11.8.2 och 11.10.1).

Vidare bör det införas regler om hur länge uppgifter, som har inhämtats med stöd av reglerna om hemlig teleavlyssning eller hemlig teleövervakning, får bevaras i avvaktan på att en annan stat som har begärt frysning kommer in med en framställning om att få ut uppgifterna. En sådan regel hör naturligen hemma i lagen om internationell rättslig hjälp. Den frågan tas upp i avsnitt 11.9.2.

Konventionen (artiklarna 17, 29 och 30) kräver att vissa trafikuppgifter beträffande särskilt utpekade meddelanden skall vara åtkomliga genast. Detta aktualiserar frågan om operatörerna skall åläggas att, redan innan det finns ett domstolsbeslut, lämna ut sådana uppgifter, om de omfattas av ett frysningsbeslut.

Att lämna ut vissa uppgifter i förtid, innan det ännu står klart om domstolen meddelar tillstånd till tvångsmedlet, skulle strida mot de grundläggande principerna för hemliga tvångsmedel. Det är också en viktig beståndsdel i bestämmelserna om frysning av elektronisk kommunikation att uppgifterna visserligen bevaras men inte röjs utan domstolsbeslut. Vidare kan det lätt uppstå tillämpningsproblem om operatörerna skulle åläggas att skilja ut vissa uppgifter bland det som har bevarats och lämna ut enbart dem. Det skulle sannolikt bli svårt att avgränsa vilka uppgifter som får lämnas ut i förtid och vilka som får lämnas ut först när det föreligger ett domstolsbeslut. Operatörernas skyldighet att snabbt röja vissa trafikuppgifter bör i stället regleras i lagen om elektronisk kommunikation (se avsnitt 11.4.3 och 11.8.3).

11.5 Förbud mot att rubba bevisning i elektronisk form

11.5.1 En ny typ av föreläggande

Förslag: Det införs en regel i 27 kap. RB som gör det möjligt att temporärt förbjuda den som innehar bevisning i elektro-

nisk form att förstöra, förändra eller på annat sätt göra bevisningen oåtkomlig. Ett sådant föreläggande får inte riktas mot någon som är misstänkt. Det får inte heller avse något som inte får tas i beslag. Förbudet skall förenas med en skyldighet att bevara uppgifterna viss tid, upp till 90 dagar. Tiden för förbudet får inte bestämmas längre än nödvändigt. Om den i förbudet angivna tiden inte är tillräcklig kan förbudet förlängas genom ett nytt beslut.

Ändamålet med det nya föreläggandet

Enligt artikel 16 skall det finnas möjlighet att genom föreläggande eller på annat sätt åstadkomma snabbt säkrande av särskilt angivna lagrade datauppgifter (även trafikuppgifter), när det finns stor risk för att uppgifterna annars förändras eller går förlorade. Ett föreläggande att säkra uppgifter skall innefatta att personen åläggs att bevara uppgifterna orubbade så länge som det behövs, dock högst 90 dagar, för att behöriga myndigheter skall kunna begära att få del av dem. Vidare skall det finnas en möjlighet att ålägga personen att hemlighålla åtgärden.

Det nya tvångsmedlet frysning av elektronisk kommunikation tillgodoser kraven på ett snabbare förfarande för att säkra uppgifter om och innehållet i telemeddelanden. Frysning kan emellertid bara tillämpas på sådan information som finns hos eller befordras av operatörer. Reglerna om frysning är därför inte tillräckliga för att uppfylla kraven i artikel 16.

Den som begår dataintrång, eller som begår något annat brott med hjälp av datorsystem, använder ofta andras datorer för att sopa igen spåren efter sitt brott. Om t.ex. en hacker försöker komma in i datorer som tillhör en viktig försvarsanläggning hos en stormakt gör han det knappast med enbart hjälp av sin egen dator. Han kopplar i stället upp sig mot en eller flera olika datorer (ofta i skilda länder), som används för angreppet. På så sätt blir det svårare att spåra varifrån intrånget görs. Likaså försöker den som sprider maskar eller andra virus att dölja varifrån dessa ursprungligen kommer och utnyttjar då, ägarna ovetande, dato-

rer i andra länder. En typ av tillgänglighetsattacker förutsätter att ett flertal datorer samtidigt kontaktar den dator eller det datorsystem som är målet för attacken. Då måste gärningsmannen kunna styra många datorer, vilket som regel förutsätter intrång i dessa.

Det är inte ovanligt att svenska datorer utnyttjas på det nu beskrivna sättet. Att detta är möjligt beror ofta på att den eller de datorer som används som verktyg själva har ett svagt skydd mot angrepp.

Det förekommer också att datorer som är tillgängliga för en större krets av personer utnyttjas för IT-relaterade brott. Som exempel kan nämnas att barnpornografi har påträffats i datorer på skolor, universitet och bibliotek.

I de datorer som utan ägarens/brukarens vetskap har utnyttjats för dataintrång finns det spår som kan ge bevisning om brottet. Det är angeläget att den bevisningen kan säkras.

Vidare finns det personer som tillhandahåller tjänster på Internet men som faller utanför regleringen i 6 kap. lagen om elektronisk kommunikation. Det måste vara möjligt att snabbt kunna säkra bevisning även hos dessa.

Den som innehar lagrade data av det slag som artikel 16 reglerar kan på grund av lagregler, av tekniska skäl, av hänsyn till lagringsmöjligheterna, på grund av avtal med kunder eller av något annat godtagbart skäl ha som rutin att bevara uppgifterna endast en kort tid. Det finns därför ett behov av att mycket snabbt kunna säkra bevisning i elektronisk form. Som framgått tidigare kan i och för sig husrannsakan och beslag tillämpas hos andra än operatörer. Det är emellertid långtifrån alltid möjligt att ingripa med dessa tvångsmedel tillräckligt snabbt. Reglerna om husrannsakan är knutna till undersökningen av en fysisk plats eller ett fysiskt föremål. Även om bevisningen, med hjälp av uppgifter från en eller flera operatörer, kan spåras till en viss dator kan det ta tid att få fram var datorn rent fysiskt finns. Ett större företag eller en myndighet kan ha datorer som är sammankopplade i nät men fysiskt placerade på helt skilda adresser. Den enskilda datorn måste då spåras med hjälp av företagets eller myndighetens

IT-funktion. Både i det nu angivna exemplet och i andra fall kan det däremot vara möjligt att kontakta den som råder över systemet eller datorn, t.ex. via elektronisk post. Det kan vidare, oavsett om det är känt var informationen finns, vara svårt att någorlunda snabbt få fram expertis som kan undersöka datorn och ta till vara bevisningen. Till detta kommer att vissa uppgifter, t.ex. loggar över datakommunikation, ofta bara bevaras en kort tid. Om uppgifterna inte säkras tillräckligt snabbt finns det en påtaglig risk att de helt går förlorade. Det måste därför finnas möjlighet att snabbt ingripa för att förhindra att den bevisning som skall tas i beslag förstörs. En regel om skyldighet att bevara lagrade data skall därför inte ses som ett misstroende utan enbart som ett sätt för de brottsbekämpande myndigheterna att snabbt säkra bevisning som annars kan gå förlorad enbart på grund av rutinmässig utrensning av uppgifter.

Den svenska lagstiftningen om förundersökning och bevisning i brottmål utgår från delvis andra förutsättningar än vissa motsvarande utländska förfaranden. Vi har t.ex. inte några regler som innebär att enskilda är skyldiga att bidra med bevisning. Det är visserligen inte uteslutet att använda reglerna om edition vid brottsutredning (23 kap. 14 § andra stycket och 38 kap. 2 § RB), men enligt förarbetena är editionsreglerna inte avsedda att användas i förundersökning om brott utan i domstolsprocessen. Detta kan för övrigt också utläsas av reglernas systematiska placering i balken. Härtill kommer att editionsföreläggande under förundersökning inte får riktas mot någon som är misstänkt. Föreläggande om edition kan över huvud taget inte utfärdas innan det finns någon som är skäligen misstänkt (se NJA 2003 s. 107). Dessa grundläggande förutsättningar begränsar tillämpningsområdet för edition i brottmål avsevärt. Reglerna om husrannsakan och beslag tillkom för att på förundersökningsstadiet skapa en motsvarighet till reglerna om edition (SOU 1938:44 s. 413). Härtill kommer att det enda ändamålet med edition är att framtvinga bevisning. Edition kan därför, i motsats till beslag, inte användas som ett förstadium för förverkande. Ett av syftena

med säkringsåtgärder enligt artikel 19 punkt 3 d är att de skall kunna användas som ett förstadium för förverkande.

Det är mot den nu angivna bakgrunden inte lämpligt att basera en ny regel som är avsedd att användas för spaning mot misstänkta och utredning av brott på reglerna om edition. I stället bör man, på samma sätt som när det gäller frysning, söka en lösning som knyter an till de befintliga reglerna om tvångsmedel under förundersökning. En möjlighet kan då vara att på dataområdet skapa en motsvarighet till den möjlighet som finns att förbjuda någon att rubba fysiska bevisföremål. Medan beslag förutsätter att det är ett föremål som skall tas om hand, dvs. att det är fråga om lös egendom, finns det i 27 kap. 15 § RB ett tvångsmedel som i huvudsak är avsett att tillämpas på fast egendom. Enligt nämnda paragraf kan, för säkerställande av utredning om brott, en byggnad eller ett rum stängas till, tillträde till visst område förbjudas eller förbud meddelas mot att visst föremål flyttas eller att annan sådan åtgärd vidtas. Med stöd av den regeln kan brottsutredande myndigheter t.ex. förhindra att ett fartyg eller ett fordon som har varit inblandat i en händelse som utreds i form av en förundersökning rubbas innan det har hunnit undersökas.

Man kan i princip se ett rubbande – eller förstörande – av bevisning i elektronisk form på samma sätt som motsvarande handlande när det gäller fysiska bevisföremål. Det skulle därför inte vara främmande för svensk rätt att införa en regel om förbud mot att rubba elektronisk bevisning. En annan sak är att en regel om förbud att förstöra eller på annat sätt förhindra tillgång till elektroniska data måste formuleras på ett annat sätt.

Vad skall föreläggandet avse?

Förbudet skall avse lagrade data, dvs. historiska uppgifter. Det nya tvångsmedlet är således inte avsett att kunna användas för att fortlöpande samla in bevisning. Konventionens syfte är inte heller att ställa ökade generella krav på den som innehar uppgifter av nu aktuellt slag, t.ex. i fråga om lagringstid och liknande. Det

avgörande för om ett beslut om förbud mot rubbande skall kunna utfärdas är alltså att det existerar lagrad datainformation som behövs för säkerställande av utredningen om det brott som förundersökningen avser.

Vidare skall det röra sig om information som den mot vilken förbudet riktas har i sin besittning eller som denne på annat sätt har kontroll över. Om den information saken rör visserligen är lagrad någon annanstans inom landet men den förelagde har direkt åtkomst till denna t.ex. via terminal får denne anses ha kontroll över informationen.

Förbudet mot att rubba bevisning bör ha formen av ett föreläggande som anger dels vilken bevisning det är fråga om, dels hur den förelagde skall uppfylla kravet. Det bör nämligen vara möjligt att uppfylla kravet på att bevisningen skall förbli orubbad på i princip två olika sätt. Det ena är att förhindra förändring och radering av samt åtkomst till den elektroniska bevisningen, men låta den finnas kvar på sin ursprungliga plats. Det andra är att säkra informationen genom en kopia som senare överlämnas till behörig myndighet.

För den enskilde är det en mindre ingripande åtgärd att få ett föreläggande än att utsättas för husrannsakan. Föreläggande bör därför användas i första hand, om den åtgärden bedöms vara tillräcklig för att snabbt säkra bevisningen.

Den lagtekniska lösningen

En regel om förbud mot att rubba bevis i elektronisk form hör naturligt hemma i 27 kap. RB. Bestämmelsen bör vara generell i den meningen att den skall kunna tillämpas på alla typer av brott. Eftersom det inte ställs några krav på brottets svårhetsgrad för beslag bör inte heller någon sådan begränsning gälla för förbud mot att rubba elektronisk bevisning, som normalt utgör ett steg på vägen mot beslag. Förbud skall således kunna utfärdas oberoende av brottets svårhetsgrad.

Förbudet innebär i sig ingen skyldighet för den förelagde att också lämna ut informationen, enbart att bevara den i avvaktan

på att åklagaren antingen beslutar om husrannsakan eller tar bevisningen i beslag eller begär hos rätten att bevisningen skall lämnas ut med stöd av ett editionsföreläggande.

Det förhållandet att ett förbud mot att rubba elektronisk bevisning främst är avsett att leda fram till beslag hindrar nämligen inte åklagaren från att, om det finns rättsliga förutsättningar för det, välja att framställa yrkande om edition i stället. Med hänsyn till dels kravet på skälig misstanke dels att ändamålet med edition endast är att säkra sådant som skall användas som bevisning i process är emellertid, som tidigare nämnts, den lösningen i många fall inte användbar.

Om den förelagde självmant överlämnar bevisningen får förundersökningsledaren avgöra om den skall tas i beslag eller ej.

Mot vem får föreläggandet riktas?

Ett förbud av nu aktuellt slag bör inte kunna riktas mot någon som är misstänkt. Det skulle strida mot artikel 6 i Europakonventionen att ålägga någon att tillhandahålla bevisning mot sig själv (se SOU 2001:25 s. 168 ff och Danelius s. 233 ff angående passivitetsrätten) och mot förbudet mot self-incrimination i FN-konventionen om medborgerliga och politiska rättigheter. I artikel 15, som skall tillämpas på de processrättsliga reglerna, hänvisas till dessa båda konventioner, varför det får anses underförstått att en sådan begränsning är tillåten (se även punkt 147 i den förklarande rapporten).

Inom ramen för ett förundersökningsförfarande är det således uteslutet att använda förelägganden av detta slag mot någon som är misstänkt, oavsett på vilken nivå misstanken ligger. Det kan givetvis vara svårt att bedöma förekomsten av brottsmisstanke i ett akut läge, men i de flesta fall torde det redan från början stå klart att t.ex. ett dataintrång ursprungligen härrör från en annan dator.

Förelägganden kan riktas mot flera subjekt samtidigt, oavsett om det är samma eller olika information som finns lagrad hos dessa.

Avsikten med förbudet är, som tidigare nämnts, att sådan bevisning som löper särskild risk att snabbt gå förlorad skall säkras så att den senare kan bli föremål för beslag. Detta innebär att undantag även måste göras för de situationer där beslag inte får förekomma (se avsnitt 6.12.3 och 11.6.1). För edition tillämpas samma begränsningar som för beslag (38 kap. 2 § andra stycket RB). Det är således inte möjligt att kringgå beslagsförbudet genom ett yrkande om edition.

I ett senare avsnitt (avsnitt 11.9.3) behandlas operatörers skyldighet att lämna ut trafikuppgifter. Denna skyldighet hindrar inte att ett föreläggande riktas mot en operatör. Detta kan vara lämpligt t.ex. om det krävs ytterligare tid för att utreda om brottet når upp till den nivå som krävs för att operatören skall röja trafikuppgifterna med stöd av den nya regeln om uppgiftsskyldighet i lagen om elektronisk kommunikation. Ett föreläggande får däremot självfallet inte användas för att kringgå reglerna om hemlig teleavlyssning eller hemlig teleövervakning. I brådskande fall kan dock ett föreläggande förhindra att uppgifterna går förlorade under den tid som åtgår för överväganden huruvida frysning av elektronisk kommunikation eller annat tvångsmedel kan användas.

Innehållet i föreläggandet

Det är viktigt att föreläggandena utformas så att den förelagde inte drabbas i onödan. Förbudet skall avse en viss närmare angiven information, t.ex. loggningar under en viss tidsperiod eller en viss datafil eller någon annan på motsvarande sätt specificerad information. Generellt utformade förelägganden som ålägger någon att utan begränsning spara all information från en viss period får således inte utfärdas.

Proportionalitetsprincipen (27 kap. 1 § tredje stycket RB) skall tillämpas på föreläggandena. Inom ramen för denna skall beslutsfattaren noga avväga hur omfattande föreläggandet skall vara. Om syftet med föreläggandet kan uppnås t.ex. genom att den förelagde gör en utskrift av en logg, eller bevarar viss infor-

mation på en diskett eller en CD, bör föreläggandet inskränkas till en sådan åtgärd. Andra möjligheter att begränsa åläggandet måste alltid beaktas.

Ett föreläggande skall tidsbegränsas. Tiden får inte bestämmas längre än vad som i det enskilda fallet är nödvändigt. Som längst får ett föreläggande gälla 90 dagar. Det är emellertid möjligt att utfärda ett förnyat föreläggande. Upprepade förelägganden bör dock inte förekomma. Ett föreläggande av det nu aktuella slaget bör nämligen så snart som möjligt följas upp med beslag eller annan motsvarande åtgärd som säkrar bevisningen. Det innebär att de flesta förelägganden kommer att ha kort varaktighet. Vid internationell rättslig hjälp torde det dock inte kunna undvikas att maximitiden utnyttjas i ett eller annat fall.

11.5.2 Vem skall besluta?

Förslag: Förbud mot att rubba elektronisk bevisning skall meddelas av åklagare.

Om det inte meddelas några särskilda regler om vem som får besluta om en åtgärd av det skisserade slaget kommer beslutanderätt att tillkomma var och en som kan besluta om beslag, dvs. åklagare, annan förundersökningsledare samt, i brådskande fall, polisman (27 kap. 4 § andra stycket RB). En sådan ordning är inte lämplig, särskilt mot bakgrund av att möjligheten framför allt torde komma att användas på begäran av en främmande stat. Det förhållandet att det är fråga om en för svensk rätt ny typ av tvångsmedel, att de brottsutredningar där en fråga av detta slag kan komma att väckas regelmässigt torde vara komplicerade samt att besluten kan kräva kvalificerade juridiska överväganden talar för att beslutanderätten läggs på åklagare. Vidare ankommer det på åklagare att handlägga framställningar om rättslig hjälp. Även den omständigheten att det inom åklagarväsendet finns en organisation för beslut i tvångsmedelsfrågor utanför ordinarie tjänstetid talar för att beslut bör fattas av åklagare. Om en fråga om att använda ett föreläggande av detta slag uppkommer under en

förundersökning som leds av polisen kan åklagare ta över förundersökningsledningen med stöd av 23 kap. 3 § första stycket sista meningen RB.

Det bör, i likhet med vad som gäller för flertalet tvångsmedel, inte föreskrivas någon särskild form för beslutet. Finns det möjlighet bör beslutet vara skriftligt. Om emellertid ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande måste ett muntligt beslut om förbud kunna meddelas. Detta skall i så fall, i enlighet med Riksåklagarens föreskrifter (RÅFS 2002:1), dokumenteras i efterhand.

Den förelagde bör – oavsett om själva beslutet är muntligt eller skriftligt – så snart som möjligt få ett skriftligt bevis om beslutet. Ett huvudskäl till detta är att undanröja varje tvivel om förbudets omfattning. Ett annat viktigt skäl är att beslutet behövs för att den förelagde skall kunna få detta prövat av domstol (se nästa avsnitt). Beslutet skall därför – i likhet med ett protokoll över beslag – innehålla uppgift om vilken domstol som i förekommande fall skall pröva frågan.

11.5.3 Handläggningen m.m.

Förslag: Den som har drabbats av ett förbud mot att rubba bevisning i elektronisk form skall kunna begära rättens prövning av det. För sådan prövning tillämpas reglerna om prövning av beslag. Den som har ålagts ett förbud får även åläggas tystnadsplikt angående förbudet.

En viktig fråga är om ett förbud att rubba bevisning i elektronisk form skall kunna prövas av domstol. Det är normalt inte möjligt att överklaga ett beslut av åklagare under en förundersökning (se Förvaltningsrättslig tidskrift 2000 s. 49). Däremot finns det regler om att vissa beslut om tvångsmedel kan bringas under domstolsprövning på initiativ av den berörde. Detta gäller bl.a. beslag. Eftersom ett beslut om förbud att rubba elektronisk bevisning är ett ingrepp mot den enskilde och det är fråga om en åtgärd med viss varaktighet bör beslutet kunna underställas dom-

stol för prövning. En lämplig lösning kan då vara att knyta an till reglerna om beslag i 27 kap. 6 § RB. Den lösningen skulle innebära att den som har drabbats av ett förbud av nu aktuellt slag kan begära prövning hos domstol, som då skall hålla förhandling senast fjärde dagen efter det att begäran om prövning har kommit in till domstolen. Rättens beslut kan därefter överklagas av någon av parterna med stöd av 49 kap. 5 § 6 RB. Om rätten upphäver förbudet kan åklagaren begära inhibition, i syfte att förhindra att bevisningen går förlorad innan överinstansen har hunnit ta ställning i frågan.

En annan fråga som måste lösas är hur det krav på sekretess som finns i konventionen (artikel 16 punkt 3) skall uppfyllas.

För att en enskild person skall kunna åläggas tystnadsplikt rörande en åtgärd av detta slag krävs det en uttrycklig lagregel. Detta är emellertid inte heller något som är främmande för förundersökningsförfarandet. I 23 kap. 10 § femte stycket RB finns en regel som ger undersökningsledare möjlighet att ålägga den som har varit närvarande vid ett förhör tystnadsplikt angående vad som har kommit fram under förhöret. Om det vid en domstolsförhandling inom stängda dörrar förebringas sekretessbelagda uppgifter kan domstolen förordna om yppandeförbud (5 kap. 4 § RB). Det finns därför inget principiellt hinder mot att den som föreläggs att inte rubba bevisning i elektronisk form också förbjuds att yppa detta. En sådan bestämmelse bör lämpligen placeras i den paragraf som reglerar skyldigheten att skydda bevisningen.

Om någon bryter mot ett förbud mot att rubba bevisning kan straffansvar utkrävas enligt 17 kap. 13 § BrB för brytande av myndighets bud. Detta förutsätter givetvis att den förelagde bevisligen har fått del av föreläggandet, vilket understryker vikten av att förelägganden har skriftlig form.

Bryter något mot ett åläggande att inte yppa förbudet kan ansvar följa enligt 9 kap. 6 § RB. Eftersom yppandeförbud endast skall kunna utfärdas av åklagare bör en följdändring göras i den bestämmelsen.

11.6 Anpassning till ny teknik

11.6.1 Allmänt om behovet av nya eller ändrade regler

Behövs det nya regler?

Konventionen förutsätter att staterna skall ha adekvata regler om husrannsakan och beslag. Den tekniska utvecklingen har inneburit att det allt oftare diskuteras om de traditionella tvångsmedlen husrannsakan och beslag i dag täcker behovet av tvångsmedel för att samla bevisning i elektronisk form. När det gäller elektronisk kommunikation och hanteringen av lagrade datauppgifter är frågan om vilket eller vilka tvångsmedel som får användas av avgörande betydelse. För skilda tvångsmedel gäller olika regler om bl.a. brottets svårhetsgrad, beslutsfattare, och mot vem tvångsmedlet får användas.

Frågan om reglerna om husrannsakan och beslag behöver anpassas till den moderna tekniska miljön har, som tidigare nämnts, utretts av Datastraffrättsutredningen. Utredningen, som lade fram sitt betänkande år 1992, föreslog omfattande ändringar såväl inom straffrätten som inom processrätten, i syfte att anpassa regelsystemen till den alltmer utbredda digitaliseringen. Förslagen innebar bl.a. att TF:s handlingsbegrepp, som omfattar även elektroniska och andra upptagningar, skulle införas i RB. Husrannsakan skulle enligt förslaget omfatta lagringsutrymmen för data, varvid det tekniska skyddet för datainformationen skulle jämställas med ett fysiskt. Förslagen har inte lett till någon lagstiftning och anses numera vara föråldrade i de flesta delar (se Ds 2003:29 s. 38).

Polisrättsutredningen, som hade till uppgift att se över reglerna i 27 och 28 kap. RB, ansåg att polisens förfarande att söka efter information i datorer saknar lagstöd (SOU 1995:47 s. 184 f). Utredningen, som menade att förfarandet bör lagregleras, lade dock inte fram något förslag till lösning (s. 192).

IT-utredningen menade däremot – utan att redovisa några skäl för sitt ställningstagande – att reglerna i 27 och 28 kap. RB är

direkt tillämpliga på datainformation (SOU 1996:40 s. 209). Frågan kommenterades inte i det fortsatta lagstiftningsarbetet.

Inte heller Polisrättsutredningens förslag har lett till någon lagstiftning. Statsmakterna har därför inte tagit ställning till huruvida de nuvarande reglerna om husrannsakan och beslag är tillräckliga när det gäller möjligheterna att söka efter och säkra information i elektronisk form. I propositionen om intrångsundersökning (prop. 1998/99:11 s. 40) noterade regeringen dock, under hänvisning till Polisrättsutredningens betänkande, att polisens befogenheter att vid en husrannsakan söka efter uppgifter som är lagrade i datorer inte är närmare reglerade.

Sedan dessa betänkanden lades fram har situationen komplicerats ytterligare. Ett skäl till detta är att den nya tekniken leder till att olika former av kommunikation blir alltmer integrerade med varandra. Datorer kan användas för telefoni, mobiltelefoner kan kopplas till datorer för att ta emot telefax och datorkommunikation kan användas för att sända över bilder, för att nu bara ta några exempel. De traditionella kommunikationssätten telefoni och postbefordran används parallellt med motsvarande elektroniska kommunikationstjänster. Tvångsmedelsregleringen bygger emellertid alltjämt i stor utsträckning på den äldre tekniken och på att det finns tydliga gränser mellan olika kommunikationssätt.

Konventionen kräver att parterna ser över sina straffprocessuella bestämmelser, så att dessa anpassas till modern IT-miljö. Det förutsätts t.ex. att husrannsakan och beslag skall kunna tillämpas på datorbehandlingsbara uppgifter, även om dessa inte har omvandlats till fysisk form, eller att det skall finnas liknande tvångsmedel med den funktionen (artikel 19 punkterna 1 och 3). Det har lämnats till de enskilda staterna att närmare avgöra hur anpassningen skall ske. Konventionen förutsätter vidare att befintliga och nya tvångsmedel skall tillförsäkra den enskilde grundläggande rättssäkerhetsgarantier (artikel 19 punkt 5). Dessa skall avspegla den balans som krävs mellan brottsbekämpande myndigheters möjlighet att ingripa med effektiva medel och den enskildes rätt till skydd.

I detta avsnitt behandlas frågan om anpassning av reglerna om kvarhållande av post, husrannsakan och beslag.

Elektronisk post

När regleringen av hemlig teleavlyssning och hemlig teleövervakning gjordes teknikneutral i mitten av 1990-talet infördes begreppet telemeddelande. Det omfattar, som tidigare nämnts, såväl textmeddelanden som bilder, ljudöverföring och traditionella telefonitjänster. Syftet med ändringen var att så långt möjligt skapa en teknikneutral reglering. Effekterna av de senaste årens utveckling inom datorkommunikation och mobiltelefoni, i kombination med att de flesta numera har tillgång till datorer och mobiltelefoner, har lett fram till att kommunikation generellt sett i allt större utsträckning äger rum i elektronisk form. Det har vidare tillkommit helt nya tjänster inom bl.a. området för mobiltelefoni, t.ex. SMS (Short Message Service), som är textmeddelanden som utgör telemeddelanden, och MMS (Multi Media Messaging Service), som endast skiljer sig från SMS på det sättet att man även kan bifoga ljud- och bildfiler.

Meddelanden som överförs elektroniskt har i dag ett starkare skydd än motsvarande meddelanden som överbringas med traditionella kommunikationssätt, i och med att de räknas som telemeddelanden. Som exempel kan nämnas att innehållet i elektronisk post som är under befordran enbart är åtkomligt genom ett beslut om hemlig teleavlyssning, vilket i princip förutsätter ett brott med minst två års fängelse i straffskalan eller försök, förberedelse eller stämpling till ett sådant brott. Ett brev med samma innehåll som sänds med traditionell post kan däremot tas i beslag under förutsättning att det är föreskrivet fängelse i ett år eller mer för brottet och att brevet hade kunnat tas i beslag hos mottagaren. Motsvarande gäller paket och andra försändelser. Ett annat exempel på hur de nuvarande reglerna fungerar är att om barnpornografiska bilder skickas som en bilaga till elektronisk post är hela innehållet ett telemeddelande. Det innebär att det med dagens reglering inte är möjligt att ta del av innehållet så

länge det är under befordran, eftersom straffskalan för barnpornografibrott är för låg för hemlig teleavlyssning. Sänds bilderna däremot med vanlig postbefordran kan försändelsen dels kvarhållas, dels tas i beslag. En videofilm med barnpornografiskt innehåll som i oförändrat skick förs över till datormedium kan således sändas som en datafil till en annan person utan att de brottsbekämpande myndigheterna har någon möjligt att ingripa med tvångsmedel eftersom den överförs elektroniskt, medan videofilmen kan kvarhållas och tas i beslag om den postas. Dessa skillnader är enbart en konsekvens av att meddelanden i elektronisk form räknas som telemeddelanden, när de är under befordran, och att de därmed har samma starka skydd som exempelvis telefonitjänster.

Den föreslagna utvidgningen av tillämpningsområdet för hemlig teleövervakning till att omfatta även barnpornografibrott och dataintrång är ett viktigt steg för att effektivisera bekämpningen av dessa brottstyper. Det bör emellertid framhållas att utvidgningen inte leder till ökade möjligheter att ta del av innehållet i meddelandet. Den innebär endast att det är möjligt att få fram bevisning exempelvis om att det har förekommit kommunikation mellan två datorer, när den har ägt rum, hur länge den har pågått och hur stor mängd material som har utväxlats. Däremot är det inte möjligt att få reda på om t.ex. sändningen har omfattat förbjudna pornografiska bilder eller annat otillåtet material, eftersom hemlig teleövervakning inte omfattar innehållet i telemeddelanden. I de fall där det som har sänts har lagrats antingen i den avsändande eller i den mottagande datorn är innehållet emellertid åtkomligt med straffprocessuella tvångsmedel hos avsändaren eller mottagaren.

I takt med att allt fler meddelanden sänds elektroniskt minskar värdet av reglerna i 27 kap. 3 § (beslag av brev eller annan försändelse under befordran) och 9 § RB (kvarhållande av försändelse; i dagligt tal kallad postkontroll).

De brottsbekämpande myndigheternas möjligheter att få del av innehållet i viss korrespondens är alltså beroende av vilken kommunikationsform som avsändaren väljer; elektronisk beford-

ran eller traditionell postbefordran. Det är svårt att finna något sakligt skäl till att information av exakt samma slag skall ha olika skydd beroende på vilket kommunikationssätt som väljs. En sådan skillnad torde inte heller har varit avsedd av lagstiftaren. I prop. 1988/89:124 påpekade departementschefen att de utvidgade reglerna om hemlig teleavlyssning i och för sig kunde motivera att man såg på frågan om brytande av brevhemlighet på ett nytt sätt (s. 40). Hon ansåg dock att man borde avvakta utvecklingen innan man tog upp sådana övergripande frågor. Någon översyn med inriktning på skillnaderna mellan regleringen av elektronisk post och annan post har emellertid inte kommit till stånd.

Elektronisk post används i dag inte bara som en ersättning för traditionell post, dvs. för att skicka meddelanden mellan två individer. Den används ofta för att sända meddelanden till flera personer samtidigt. Den är dessutom ett snabbt och billigt sätt att ordna massutskick, något som är av särskild betydelse vid spridning av något som i sig är straffbelagt. För en närmare beskrivning av den elektroniska postens utveckling se SOU 2001:28 s. 147 ff.

Den explosionsartade utvecklingen av bl.a. elektronisk post och Internetanvändning kunde knappast förutses. Enligt uppgift förmedlar enbart en av Internet-operatörerna i Sverige ca 20 miljoner e-postbrev varje dygn. Samtidigt har den traditionella postbefordran minskat kraftigt. Detta aktualiserar frågan om man bör öka möjligheterna att kontrollera elektronisk post, särskilt mot bakgrund av att detta kommunikationssätt blir allt vanligare vid vissa brottstyper.

Husrannsakan i IT-miljö

Reglerna om husrannsakan är utformade för att tillgodose de brottsutredande myndigheternas behov av att undersöka rum, byggnader och andra sådana utrymmen samt olika typer av fysiska föremål, däribland slutna förvaringsutrymmen såsom kassaskåp, lådor, skrin och liknande. Husrannsakan tar med andra ord

sikte på fysiska miljöer och på undersökning av fast eller lös egendom.

Med tiden har det blivit allmänt accepterat att reglerna om husrannsakan kan tillämpas även på datorer. Det råder emellertid fortfarande skilda meningar både om huruvida reglerna om husrannsakan och beslag i sig är tillämpliga på den information som är lagrad i dessa och om hur de skall tillämpas. Som framgått av den tidigare redovisningen har flera statliga utredningar inom loppet av några få år kommit till helt olika slutsatser i dessa frågor.

I kommentaren till rättegångsbalken framhålls det att datorer normalt är placerade i sådana miljöer, dvs. hus och rum, som inte får genomsökas utan ett beslut om husrannsakan, varför det blir en sekundär fråga hur man skall se på undersökningen av själva datorn (Peter Fitger, Rättegångsbalken, s. 28:7). Att undersöka en dators innehåll utan ett föregående beslut om husrannsakan torde därför mycket sällan vara lagligen möjligt. Har husrannsakan ägt rum och datorn har tagits i beslag kan det beslagtagna undersökas. Den närmare innebörden av detta finns det emellertid också delade meningar om.

Det är utan tvekan svårt att överföra traditionella rumsbegrepp till en teknisk miljö som inte har samma fysiska gränser som de miljöer som bestämmelsen om husrannsakan har tillskapats för. I IT-miljö jämställer man ofta de logiska spärrar som skapas genom olika tekniska lösningar med fysiska gränser. Genom behörighetskort, åtkomstkoder, lösenord och liknande spärrar skapas ”slutna” förvaringsutrymmen för informationen, oavsett var i världen denna rent faktiskt lagras respektive är åtkomlig. Det är emellertid inte självklart att man kan dra paralleller mellan fysiska gränser och tekniska spärrar av olika slag. Om man gör det kommer tvångsmedelsanvändningen att bli helt beroende av varierande tekniska förutsättningar, inte av de gränser som lagstiftaren ställer upp. Mot den bakgrunden bör övervägas hur husrannsakan i IT-miljö skall vara reglerad.

Datainformationens immateriella natur innebär vidare att gränsen mellan husrannsakan och beslag inte är lika tydlig som

när tvångsmedlen tillämpas i fysisk miljö på föremål. Eftersom det gäller olika förutsättningar för att få använda tvångsmedlen, bl.a. olika krav på brottets svårhetsgrad och på brottsmisstanke, är det olyckligt att gränsen mellan tvångsmedlen inte är klart utstakad.

Det är emellertid inte bara tillämpligheten av reglerna om husrannsakan som behöver diskuteras. Ett typiskt exempel på frågor som anses olösta är om, och i så fall i vilken utsträckning, det är tillåtet att genomföra en husrannsakan enbart med tekniska hjälpmedel utan hänsyn till var den dator som skall undersökas befinner sig, alltså en form av husrannsakan på distans.

En annan aspekt på samma fråga är vilken betydelse det har att t.ex. företag inte sällan lagrar sin datainformation utomlands. Från en dataterminal kan man ta fram information som är lagrad var som helst i världen. Om lagring i ett annat land är billigare eller av annat skäl lämplig finns det numera inga tekniska hinder mot det. I vissa fall hindrar dock lagstiftningen lagring i annat land.[41] De brottsutredande myndigheternas möjligheter att ta del av information som är lagrad utomlands begränsas av att svensk myndighetsutövning inte får bedrivas på en annan stats territorium. Är informationen lagrad utomlands är myndigheterna därför hänvisade till att begära internationell rättslig hjälp för att få fram informationen. Detta gäller självfallet inte om det är fråga om sådan information som är tillgänglig för alla, t.ex. information som gjorts allmänt tillgänglig på Internet. En fråga som detta väcker är om sådant material som lagras utomlands kan hämtas in med samtycke av den berörde.

En närliggande fråga är i vilken utsträckning som brottsbekämpande myndigheter har rätt att ta del av datauppgifter som i och för sig är allmänt tillgängliga, t.ex. på en hemsida, men där innehavaren har förklarat att sidan inte står öppen för exempelvis polis och åklagare. Frågan är om den enskilde genom en så enkel åtgärd skall kunna hindra brottsbekämpande myndigheter från att ta del av informationen.

[41] Det finns t.ex. särskilda regler om förvaring av bokföringsmaterial utomlands.

Beslag

Beslagsreglerna tar, som tidigare nämnts, sikte på fysiska föremål. Det är således först när elektroniska data antingen har omvandlats till en utskrift eller har lagrats på ett fysiskt medium som beslagsreglerna kan träda i funktion. Husrannsakan som syftar till att få fram elektroniska data får därmed det vidare syftet att inte bara göra informationen tillgänglig utan även att omvandla den i sådan form att beslagsreglerna kan tillämpas. Man kan naturligtvis diskutera om omvandlingen i stället utgör ett led i beslagsförfarandet. Eftersom reglerna om husrannsakan innehåller strängare krav än reglerna om beslag är det från rättssäkerhetssynpunkt förmånligare för den enskilde att se omvandlingen som ett led i husrannsakan. Det synsättet är också bäst förenligt med den grundläggande förutsättningen för beslag, nämligen att föremålet för beslaget skall vara tillgängligt.

Eftersom beslagsreglerna utgår från traditionella informationsbärare, samtidigt som information i allt större utsträckning datorbehandlas och lagras i elektronisk form, har det uppstått en klyfta mellan regelsystemet och verkligheten. I 27 kap. 1 § andra stycket RB föreskrivs att reglerna om beslag inte bara gäller föremål utan även skriftliga handlingar, om inte annat är föreskrivet. Syftet med regeln är att göra klart att en handling får tas i beslag även om det bara är den information som handlingen innehåller som är av intresse, inte handlingen som sådan. I 2 § följs detta upp med regler som i vissa fall förbjuder beslag. Om handlingens innehåll kan antas vara sådant att någon inom de kategorier som räknas upp i 36 kap. 5 § RB (bl.a. läkare, advokater, sjuksköterskor och psykologer) inte får höras som vittne om innehållet i handlingen och handlingen innehas av denne eller av den till vars förmån tystnadsplikten gäller, får handlingen inte tas i beslag. Vidare får meddelanden mellan den misstänkte och hans närstående eller hans närstående emellan bara tas i beslag vid mycket grova brott.

Enligt sin ordalydelse gäller beslagsförbuden bara när det är fråga om en traditionell handling, inte när informationen är lagrad på datamedium. Enligt uppgift tillämpas inte heller alltid re-

geln om beslagsförbud när beslag görs av datorlagrad information. Vissa anser att reglerna om beslagsförbud skall tillämpas analogt medan andra menar att det inte behövs. Detta innebär att, genom den tekniska utvecklingen, har skyddet för exempelvis läkarjournaler i elektronisk form, en advokats klienthandlingar som är lagrade på datamedium eller en tidningsredaktions material som inte är i pappersform blivit betydligt bräckligare än vad lagstiftaren har avsett, eftersom regeln om beslagsförbud inte har anpassats till den numera dominerande tekniska formen för framställning och lagring av text.

Frågan om kopiering av beslag tas upp i ett särskilt avsnitt (11.6.5).

11.6.2 Kvarhållande av elektronisk post

Förslag: En regel om kvarhållande av elektronisk post införs. Den utformas efter mönster av regeln om kvarhållande av traditionell post. Vidare görs regeln om beslag av brev och andra försändelser under befordran tillämplig på elektronisk post. Det innebär att det införs en möjlighet att ”hålla kvar” en kopia av ett elektroniskt meddelande, i syfte att åklagare skall kunna ta ställning till om meddelandet skall tas i beslag. Beslut om kvarhållande skall fattas av domstol på yrkande av åklagare. Beslag av elektronisk post får endast förekomma om det för brottet är föreskrivet fängelse i ett år eller däröver. Med den föreslagna regleringen skapas generellt bättre förutsättningar att utreda brott.

En ny regel om kvarhållande av elektronisk post

Den tekniska utvecklingen har successivt urholkat de brottsbekämpande myndigheternas möjligheter att använda postkontroll som ett led i brottsutredningar, i och med att kommunikation numera till allt större del sker elektroniskt. Detta är som framgått ovan en konsekvens av att elektronisk post definieras som

ett telemeddelande och följer de regler som ursprungligen var avsedda enbart för telefonitjänster. Den lösning som har valts i den svenska lagstiftningen har lett till att skyddet för elektronisk post har blivit betydligt starkare än vad som är motiverat med hänsyn till meddelandets karaktär. Man kan med fog fråga sig om ett meddelande skall ha ett starkare skydd enbart därför att det sänds elektroniskt.

För ett drygt decennium sedan fanns det knappast något praktiskt behov av kunna kontrollera elektronisk post. Varken privatpersoner eller företag använde elektronisk post i den utsträckning som nu är fallet. Det är därför inte förvånande att lagstiftaren ville avvakta den framtida utvecklingen. I dag är förhållandena emellertid annorlunda. Nu finns det dels ett stort praktiskt behov, dels en större förståelse för att de brottsbekämpande myndigheterna måste ha tillgång till tvångsmedel som är anpassade till dagens teknik, vilket inte minst den nyligen antagna propositionen om utvidgat tillämpningsområde för de hemliga tvångsmedlen visar. Det är också välkänt bland dem som använder elektronisk post att tekniken inte garanterar att utomstående inte får tillgång till elektroniska meddelanden. Den som använder detta kommunikationssätt tar alltid en risk att meddelandet kan komma i orätta händer, på samma sätt som den som skriver ett vykort inte kan gardera sig mot att någon utomstående tar del av innehållet.

En regel om kontroll av elektronisk post skulle underlätta anpassningen till konventionen om IT-relaterad brottslighet. Konventionens utgångspunkt är att det generellt skall vara möjligt både att tillfälligt säkra uppgifter om elektronisk kommunikation och att genom husrannsakan och beslag slutligt säkra uppgifterna för bevisändamål. I det perspektivet är det en nackdel att vår lagstiftning har en vidsträckt definition av vad som är ett telemeddelande i kombination med en reglering som innebär att endast hemlig teleavlyssning och hemlig teleövervakning får användas för att hos operatörer hämta in uppgifter om sådana meddelanden. Medan hemlig teleavlyssning och hemlig teleövervakning förutsätter att brottet har ett visst minimistraff kräver

reglerna om kvarhållande och beslag av försändelse under befordran att det för brottet är föreskrivet fängelse i ett år eller däröver. Åtskilliga av de brott som inte har ett tillräckligt minimistraff för hemlig teleavlyssning eller hemlig teleövervakning har däremot ett straffmaximum på ett års fängelse eller mer. Så är fallet med alla de brott som hänför sig till konventionens artiklar 2-11, utom vissa ringa brottsformer.

Om man i större utsträckning likställer elektronisk post med post av traditionellt slag kan man således vinna stora fördelar ur brottsbekämpningssynpunkt. Frågan är då om en sådan förändring är godtagbar från andra utgångspunkter. Som redovisats tidigare innehåller både regeringsformen och Europakonventionen regler till skydd för korrespondens. Skyddet kan emellertid begränsas genom lag. En sådan begränsning får göras bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får inte heller gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte sträcka sig så långt att den blir ett hot mot den fria åsiktsbildningen.

Det är lagtekniskt möjligt att införa regler om kontroll av elektronisk post, utan att rubba den grundläggande principen om att meddelanden under befordran av ett post- eller teleföretag skall ha särskilt skydd. Om man väljer samma konstruktion för kontroll av elektronisk post som för kontroll av traditionell post, dvs. ställer lika stränga krav i fråga om brottets svårhetsgrad, och tillskapar motsvarande rättssäkerhetsgarantier i form av domstolsbeslut, torde inte några principiella invändningar kunna resas mot tvångsmedlet.

En viktig fråga är hur man skall avgränsa bestämmelsens tillämpningsområde eftersom elektronisk post kan förekomma i olika skepnader. Elektronisk post är ofta en tjänst som ingår i ett Internetabonnemang. Det kan också vara en webbaserad tjänst, där mottagaren av den elektroniska posten kan läsa denna genom att gå in på webbsidan.

Begreppet elektronisk post är inte definierat i lagen om elektronisk kommunikation. Däremot har det nyligen införts en ny

reglering i syfte att begränsa oönskad e-postreklam. Som ett led i detta har det i marknadsföringslagen införts en definition av elektronisk post. Enligt denna avses med elektronisk post ett adresserat eller på annat sätt individualiserat elektroniskt meddelande i form av text, röst, ljud eller bild som sänds via ett allmänt kommunikationsnät och som kan lagras i kommunikationsnätet eller i mottagarens terminalutrustning till dess mottagaren hämtar det. Definitionen bygger på ett EU-direktiv om integritet och kommunikation. Eftersom den i direktivet angivna definitionen ansågs alltför vid, fann regeringen det nödvändigt att precisera begreppet genom en särskild definition (se prop. 2003/04:43 s. 14).

Syftet med det nya tvångsmedlet skall vara att kunna fånga upp elektronisk post riktad till individer för kontroll av om den skall tas i beslag. Den definition som har valts i marknadsföringslagen kan därför tjäna som en utgångspunkt. Någon motsvarande definition bör dock inte införas i rättegångsbalken.

Kontroll av elektronisk post bör omfatta endast sådan elektronisk post som ingår i en kommunikationstjänst som regleras i 6 kap. lagen om elektronisk kommunikation. En förutsättning är nämligen att det finns en operatör som kan ombesörja att domstolens beslut verkställs.

Vidare bör det vara fråga om telemeddelanden adresserade till en viss individ. Detta är ett grundläggande krav för att rättens beslut skall kunna verkställas. I likhet med vad som är fallet med kontroll av traditionell post bör det inte krävas att mottagaren är misstänkt. Däremot skall förundersökningen avse misstanke om ett brott för vilket det är föreskrivet fängelse ett år eller mer (jfr 27 kap. 3 § RB). Vidare skall meddelandet kunna tas i beslag hos mottagaren. Det sistnämnda innebär dels att de grundläggande kraven för beslag skall vara uppfyllda, dels att något beslagsförbud inte är tillämpligt.

En särskild fråga är var den nya regeln bör placeras. En möjlighet är att ha regler om kvarhållande av traditionell post och elektronisk post i samma paragraf. Fördelen med detta är att det inte i samma utsträckning krävs följdändringar i annan lagstift-

ning som exempelvis lagen om elektronisk kommunikation. Nackdelen är att det finns praktiska skillnader mellan traditionell och elektronisk post, vilket ställer krav på olika lösningar. Regleras båda slagen av post i samma paragraf blir den såväl omfattande som tekniskt komplicerad. Mot den bakgrunden bör regler om kvarhållande av elektronisk post placeras i en särskild paragraf i 27 kap. RB.

Vem skall besluta?

I likhet med vad som gäller för kvarhållande av traditionell post bör av rättssäkerhetsskäl beslut om kvarhållande av elektronisk post fattas av domstol.

Framställning om kvarhållande av elektronisk post bör göras av åklagare. Det är fråga om ett nytt tvångsmedel, som har likheter med de hemliga tvångsmedlen på teleområdet, vilka alltid hanteras av åklagare. Härtill kommer att det är åklagare som i dag handhar framställningar om kvarhållande av traditionell post (se nedan). Mot den bakgrunden bör endast åklagare kunna göra framställning om kvarhållande av elektronisk post.

Beslut om kvarhållande

Domstolen skall i ett beslut om kvarhållande av traditionell post ange för vilken tid tillståndet gäller. Den längsta tillåtna tiden är en månad. Beslutet skall därefter delges berört befordringsföretag och gäller sedan från delgivningen. I fråga om beslut om hemliga tvångsmedel på teleområdet – som ursprungligen var konstruerade på samma sätt – har en annan modell valts. Beslutets giltighetstid är inte längre knuten till att det delges, utan domstolen anger direkt i beslutet hur länge detta gäller. Samma lösning bör väljas för beslut om kvarhållande av elektronisk post. Härigenom kan man också undvika ett formellt delgivningsförfarande.

Av lagtexten bör vidare framgå att tiden för kvarhållande av elektronisk post inte får bestämmas längre än vad som i det enskilda fallet är nödvändigt. En sådan regel krävs för att Sverige skall kunna leva upp till kraven i artikel 14 på grundläggande rättssäkerhetsgarantier.

I regeln om kvarhållande av traditionell post, som i sak är oförändrad sedan rättegångsbalken tillkom, finns det inte något krav på att tvångsmedlet skall upphöra i förtid om skälen för tvångsmedlet upphör. En sådan situation kan uppkomma exempelvis om det är en enda försändelse som är av intresse och denna fångas upp i början av tillståndstiden eller om den som beslutet riktar sig mot grips. Med nutida krav på rättssäkerhet torde en regel som uttryckligen anger att tvångsmedlet skall upphöra så snabbt som möjligt vara nödvändig. För att ett beslut om kvarhållande av elektronisk post skall kunna upphöra så snart det inte längre finns skäl för åtgärden bör inte bara rätten utan även åklagaren kunna häva ett beslut om kvarhållande (jfr 27 kap. 23 § RB).

Verkställighetsfrågor

Verkställigheten av ett beslut om kvarhållande av elektronisk post bör i princip kunna ske på samma sätt som vid motsvarande tvångsmedel för traditionell post, bara med den skillnaden att det i det ena fallet rör sig om kontroll av fysiska föremål och i det andra av telemeddelanden.

När det kommer in ett meddelande till en adress för elektronisk post bör en kopia av meddelandet temporärt kunna hållas kvar, i avvaktan på att åklagaren tar ställning till om det skall tas i beslag.

En viktig fråga är hur man skall se på det förhållandet att kvarhållande av elektronisk post enbart kan resultera i att en kopia av meddelandet tas i beslag, eftersom den digitala miljön inte har original och kopior i traditionell mening (se närmare om detta i Ds 2003:29 s. 103 ff). Förfarandet med kopior skiljer sig emellertid inte från det som tillämpas i fråga om kvarhållande av tra-

ditionell post (se SOU 1995:47 s. 422 f). Det utgör således inte något hinder. Frågan om kopiering behandlas närmare i avsnitt 11.6.5.

Ansvaret för verkställigheten av tvångsmedlet bör, i likhet med vad som är fallet med hemlig teleavlyssning och hemlig teleövervakning, anförtros åt Säkerhetspolisen (se avsnitt 11.4.5).

När det gäller operatörernas roll kan konstateras att eftersom elektronisk post är en form av telemeddelande finns det redan i dag regler om anpassningsskyldighet, om hur kostnaderna för verkställigheten skall fördelas samt om tystnadsplikt. En smärre lagteknisk justering av bestämmelserna i lagen om elektronisk kommunikation torde dock krävas (se avsnitt 11.10.1).

Förhållandet mellan det nya tvångsmedlet och de befintliga

En fråga som uppkommer om man inför en ny regel om kvarhållande av elektronisk post är hur detta tvångsmedel förhåller sig till hemlig teleövervakning. Eftersom elektronisk post definitionsmässigt är ett telemeddelande kan man få uppfattningen att förslaget innebär att tvångsmedlen kommer att överlappa varandra. Så blir emellertid inte fallet. Ändamålen med tvångsmedlen skiljer sig. Vid hemlig teleövervakning är ändamålet att under en viss angiven tid – framåt eller bakåt i tiden – få uppgift om all kommunikation som förekommer till och från en viss teleadress, men däremot inte att säkra innehållet i denna kommunikation. För att i realtid säkra innehållet i sådan kommunikation krävs det beslut om hemlig teleavlyssning. Kontroll av elektronisk post syftar däremot till att fånga upp visst eller vissa meddelanden som under en angiven tid förväntas komma till en viss adress. Det bakomliggande motivet är att man härigenom skall skapa förutsättningar för att meddelandet skall kunna tas i beslag.

Däremot blir det en viss överlappning i förhållande till hemlig teleavlyssning. Ett tillstånd till hemlig teleavlyssning omfattar normalt all kommunikation till och från en viss teleadress under en angiven tid. Eftersom det inte går att förutse i vilken form kommunikationen kommer att äga rum omfattar därför ett be-

slut om hemlig avlyssning också elektronisk post. Så bör vara fallet även i fortsättningen. Att flera tvångsmedel kan tillämpas på samma objekt är emellertid inte främmande för svensk rätt. Som exempel kan nämnas hemlig teleövervakning. Ett beslut om hemlig teleavlyssning innebär att vissa teleövervakningsuppgifter automatiskt avslöjas, t.ex. uppgift om vilka teleadresser som kommunicerar med varandra och när detta äger rum. Vidare kan teleövervakningsuppgifter lämnas ut med stöd av lagen om elektronisk kommunikation. På motsvarande sätt kan beslut om beslag och kvarstad gälla samtidigt för samma föremål.

Den föreslagna lösningen står inte i strid med bestämmelserna i artikel 15 i teledataskyddsdirektivet.

Konsekvensändringar

Förslaget om kvarhållande av elektronisk post aktualiserar även frågan om modernisering i vissa avseenden av bestämmelsen om kvarhållande av traditionell post, på grund av det nära sambandet mellan dessa regler. Reglerna i 27 kap. 9 § RB är i allt väsentligt oförändrade sedan rättegångsbalken infördes år 1948 och svarar därför inte i alla avseenden mot de krav som i dag ställs på straffprocessuella tvångsmedel på grund av åtagandena i Europakonventionen.

Det bör av lagtexten i 27 kap. 9 § RB framgå att tiden för kvarhållande inte får bestämmas längre än vad som är nödvändigt. En motsvarande begränsning finns för andra perdurerande tvångsmedel. Vidare bör – av skäl som har angetts nyss – det införas en skyldighet att häva tvångsmedlet när det inte längre finns skäl för detta. Regeln bör konstrueras på samma sätt som den föreslagna regeln om kvarhållande av elektronisk post, vilket innebär att såväl rätten som åklagare skall kunna häva ett beslut om kvarhållande.

För närvarande medger lagtexten att även annan undersökningsledare än åklagare får göra framställning om kvarhållande av försändelse. Sedan decennier tillämpas emellertid den arbetsfördelningen mellan polis och åklagare att åklagare alltid övertar

förundersökningsledningen när en domstolsåtgärd aktualiseras.[42] Detta innebär att bestämmelsen om att undersökningsledare kan göra framställning om kvarhållande av försändelse är obsolet. Polisrättsutredningen, vars slutbetänkande ännu inte har lett till någon lagstiftning, föreslog att endast åklagare skall få göra framställning om kvarhållande. Utredningen ansåg att detta är en uppgift som uteslutande bör ankomma på den som uppträder som part i domstolen, dvs. åklagare (SOU 1995:47 s. 421 och 503). Det är lämpligt att genomföra utredningens förslag i detta sammanhang.

11.6.3 Ändrade regler om husrannsakan

Förslag: En ny bestämmelse om husrannsakan i IT-miljö införs. Den begränsas inte fysiskt på samma sätt som den nuvarande regeln. Ändamålen med tvångsmedlet och förutsättningarna för att använda det skall vara desamma som för husrannsakan enligt 28 kap. 1 § RB. Förutom rätten bör endast undersökningsledare eller åklagare kunna besluta om husrannsakan av nu aktuellt slag. I övrigt skall i allt väsentligt gälla samma regler som för andra former av husrannsakan, t.ex. i fråga om verkställighet, underrättelse och överklagande. En mindre justering av reglerna om verkställighet av husrannsakan krävs dock. Husrannsakan i IT-miljö skall vidare kunna verkställas via kommunikationsnät. Beslut om sådan husrannsakan fattas av rätten. Om det föreligger samtycke får även åklagare besluta om verkställighet via nät.

[42] Efter en lagändring år 1957, då polisens rätt att leda förundersökning utvidgades samtidigt som begreppet mål av enkel beskaffenhet infördes i 23 kap. 3 § RB, utfärdar Riksåklagaren och Rikspolisstyrelsen efter samråd likalydande allmänna råd om hur förundersökningsledarskapet skall fördelas mellan polis och åklagare. Se RÅFS 1997:12 och Rikspolisstyrelsens Föreskrifter och allmänna råd (FAP) 403-5.

En ny regel om husrannsakan i IT-miljö

Datastraffrättsutredningen pekade på att de straffprocessuella tvångsmedlen fortfarande präglas av de allmänna förutsättningar och den teknik som fanns för drygt femtio år sedan. Det alternativ som Datastraffrättsutredningen förespråkade innebar en direkt överföring av reglerna om husrannsakan till IT-miljö. Föremålet för husrannsakan skulle enligt utredningens förslag vara förvar av data för automatisk informationsbehandling. Förslaget fick därmed en begränsning som liknade huvudregeln om husrannsakan.

Den tekniska utvecklingen har inte bara ökat förekomsten av datorer och lagrad datainformation utan även förändrat själva datorerna. Från att ha varit enormt skrymmande maskiner som krävde särskilt anpassade miljöer har utvecklingen gått mot moderna nätverk och små bärbara datorer som kan användas var som helst. Den information som bearbetas kan lagras på helt andra ställen än där verksamheten bedrivs eller där datorutrustningen finns. Numera kan dessutom andra typer av apparater, inte bara datorer, fungera som bärare av elektronisk information. Ett vanligt exempel är moderna mobiltelefoner. Mobiltelefonin har dessutom drivit på utvecklingen mot konvergens. Även förändringar av detta slag påverkar förutsättningarna för att använda tvångsmedel. Man kan förvänta sig ytterligare förändringar inom informationstekniken även på relativt kort sikt.

Det finns därför goda skäl att reglera husrannsakan i IT-miljö i en särskild paragraf och på i huvudsak samma sätt som annan husrannsakan, men samtidigt anpassa regeln till att det inte är fråga om en traditionell fysisk miljö. Regeln bör utformas så att den inte knyter an till viss teknik.

En särskild regel om husrannsakan i viss miljö är inte någon principiellt ny lösning. Sådana regler finns redan i 28 kap. 2 a och 3 §§ RB. I de fallen är det fråga om olika typer av fysiska miljöer.

Om man inför en särskild regel om husrannsakan i IT-miljö bör denna kunna tillämpas dels på alla former av datorer och datorutrustning dels på andra fysiska bärare av elektronisk information. Regeln bör därför utformas så att den kan tillämpas vid

husrannsakan i en persondator eller i en dator som ingår i ett datorsystem eller i någon annan bärare av elektronisk information. Det innebär också att exempelvis en modern mobiltelefon kan undersökas med stöd av den föreslagna regeln. Regelns tillämpningsområde begränsas dock självfallet till elektroniska data som är lagrade i Sverige eftersom de straffprocessuella reglerna är territoriellt begränsade.

Med den valda lösningen kan övervägas om tvångsmedlet bör ges en egen benämning. Ett lämpligt namn skulle kunna vara dataspårning, eftersom tvångsmedlets syfte inte är att undersöka (=rannsaka) en viss miljö utan att spåra elektroniska data och deras ursprung. Vad som talar mot ny beteckning är att man hittills har använt samma term för olika typer av husrannsakan (i lokaler, transportmedel etc.) även om förutsättningarna i övrigt skiljer sig. Vidare är husrannsakan den term som används i andra sammanhang, inte minst i internationella överenskommelser. Framför allt det sistnämnda talar för att man bör använda beteckningen husrannsakan även för undersökning i IT-miljö.

Förutsättningarna

Syftet med husrannsakan i IT-miljö skall vara att söka efter information i elektronisk form. Om en dator behöver undersökas av något annat skäl, t.ex. som ett led i en utredning angående stöld eller skadegörelse, är regeln därför inte tillämplig.

Samma allmänna förutsättningar bör gälla för husrannsakan i IT-miljö som för annan husrannsakan. Tvångsmedlet bör således kunna tillämpas vid misstanke om brott på vilket fängelse kan följa. Det bör krävas skälig misstanke för husrannsakan hos den som är misstänkt. Även hos den som inte är skäligen misstänkt bör husrannsakan få äga rum, men det bör då, i likhet med vad som gäller enligt 28 kap. 1 § andra stycket och 2 §§ RB krävas starkare skäl. Dessa skäl kan vara antingen att brottet har förövats hos denne eller att den misstänkte har gripits där eller att det annars finns synnerlig anledning att anta att det skall anträffas något som kan tas i beslag eller något annat som bidrar till

utredningen av brottet. Synnerlig anledning skall tolkas på samma sätt som i de nyss nämnda paragraferna, dvs. att det skall finnas någon konkret omständighet som gör att det med fog kan antas att åtgärden leder till det förväntade resultatet.

Proportionalitetsprincipen (28 kap. 3 a § RB) kommer att gälla även för denna typ av åtgärd eftersom den gäller för alla typer av husrannsakan.

Samtycke till husrannsakan

En särskild fråga är om den nya regeln bör innehålla en motsvarighet till tredje stycket i 28 kap. 1 §, dvs. om det bör finnas möjlighet att företa husrannsakan med samtycke. Från principiella utgångspunkter finns det skäl som talar emot att införa en regel om samtycke, eftersom frågan om samtycke till straffprocessuella tvångsmedel är föremål för beredning efter förslag av Polisrättsutredningen. Utredningen har föreslagit att regeln om samtycke till husrannsakan skall upphävas och motiverat detta med att en sådan regel inte torde uppfylla regeringsformens krav på lagstöd för husrannsakan (SOU 1995:47 s. 148).

Konventionens artikel 32 behandlar tillgång till datorbehandlade uppgifter med samtycke. Syftet med artikeln är att skapa förutsättningar för att få tillgång till information som är lagrad utomlands utan att behöva gå vägen via internationell rättslig hjälp. Det rör sig om två typer av information; dels uppgifter som är allmänt tillgängliga, dels uppgifter som är lagrade utomlands men där någon som har åtkomst till uppgifterna och laglig rätt att röja dem för brottsutredande myndigheter frivilligt medverkar till att dessa ställs till deras förfogande. Lagring utomlands blir allt vanligare, varför det har stor praktisk betydelse om åtkomsten till sådan information kan underlättas. Mot den nu angivna bakgrunden bör trots allt den nya bestämmelsen innehålla en möjlighet till husrannsakan med samtycke. Om regeln om samtycke till husrannsakan i 28 kap. 1 § tredje stycket RB skulle upphävas får frågan tas under förnyat övervägande.

Rättegångsbalken innehåller inte några generella regler om samtycke till straffprocessuella tvångsmedel. Det anses därför oklart hur de nuvarande bestämmelserna skall tolkas, eftersom de i vissa fall tillåter samtycke, i andra fall förbjuder användning av samtycke och i åter andra fall inte tar ställning till frågan om samtycke. Det råder exempelvis olika uppfattningar om tolkningen av regeln om samtycke till husrannsakan i 28 kap. 1 §.

Enligt äldre litteratur får husrannsakan företas med stöd av samtycke även om de lagliga förutsättningarna för åtgärden inte skulle vara uppfyllda (se bl.a. Gärde s. 379). Det bör dock framhållas att dessa uttalanden gjordes innan den nuvarande regeringsformen tillkom och innan Europakonventionen direktinkorporerades i svensk rätt. Vidare måste beaktas att polisens verksamhet tidigare inte var lagreglerad.

JO anser – under hänvisning till 2 kap. 6 § RF – att ett samtycke inte befriar från de grundläggande kraven för användningen av tvångsmedlet (kraven på att det föreligger ett brott, på brottets svårhetsgrad och på att ändamålen för tvångsmedlet är uppfyllda) men att samtycke däremot kan befria från krav på styrkan i misstanken eller från krav på andra särskilda skäl för att använda tvångsmedlet (JO 1965 s. 163 och 1991/92 s. 114). I fråga om husrannsakan hos annan än misstänkt anser JO att samtycke befriar från kravet på synnerliga skäl. Polisrättsutredningen har uttryckt samma uppfattning (SOU 1995:47 s. 148). I kommentaren till rättegångsbalken hävdas däremot (utan att författaren utvecklar vad han grundar sitt resonemang på eller vad detta får för konsekvenser) att det, trots förbudet i regeringsformen, bör finnas ett större utrymme för att tillmäta samtycke till husrannsakan betydelse i de fall där den som drabbas av åtgärden har ett intresse av att denna kommer till stånd (Fitger, a.a., s. 28:9).

Oavsett hur man tolkar den nuvarande bestämmelsen bör emellertid en regel om samtycke till husrannsakan i IT-miljö ha ett något snävare tillämpningsområde än regeln i 28 kap. 1 § tredje stycket RB. Den föreslagna regeln innebär att husrannsa-

kan hos någon som inte är misstänkt kan företas med samtycke, men däremot inte hos någon som är misstänkt.

Eftersom syftet med den nu föreslagna regeln om husrannsakan är att söka efter information i elektronisk form beror den fortsatta hanteringen på vilken information som eftersöks. I vissa fall kan det vara nödvändigt att ta en dator, en del av ett datorsystem eller eventuellt hela systemet i beslag för senare undersökning. I andra fall är det tillräckligt att beslagta en fysisk databärare eller att göra en kopia av den information som påträffas.

Frågan om kopiering av filer och program m.m. samt hanteringen av sådana kopior behandlas i ett följande avsnitt (avsnitt 11.6.5).

Vem skall besluta?

Om inte några särskilda regler om beslutsbehörighet införs kommer var och en som kan besluta om husrannsakan att kunna besluta om husrannsakan i IT-miljö. Det skulle innebära att rätten, åklagare, förundersökningsledare och, i brådskande fall, en polisman kan besluta om en sådan åtgärd. Frågan är om detta är en lämplig lösning. De brott där husrannsakan i IT-miljö aktualiseras torde sällan vara av enkel beskaffenhet. Härtill kommer att det torde krävas betydligt mer grannlaga överväganden för beslut av detta slag, inte minst med hänsyn till de stora skador ett felaktigt ingripande kan leda till, än för beslut om husrannsakan i traditionell miljö. Det sagda talar för en begränsning av kretsen som får besluta. Att lägga uppgiften enbart på domstol skulle ligga i linje med vad som gäller för tvångsmedlen på teleområdet. En sådan lösning skulle emellertid innebära en kraftigare inskränkning av beslutanderätten än vad saken motiverar. Dessutom skulle domstolarnas befattning med tvångsmedel under förundersökning sannolikt öka avsevärt, vilket inte är helt oproblematiskt. Hittills har som regel åklagare beslutat om husrannsakan i IT-miljö. Detta framstår också som det lämpligaste. Åtgärder av detta slag kan emellertid aktualiseras även i förundersökningar som leds av polisen. Man bör därför inte utesluta

möjligheten av att även annan förundersökningsledare än åklagare får besluta. Däremot bör en enskild polisman inte kunna fatta ett sådant beslut. Man bör således välja den lösningen att beslut om husrannsakan i IT-miljö får fattas av domstol, åklagare eller annan undersökningsledare.[43]

Om saken inte är brådskande bör, på samma sätt som vid annan husrannsakan, rätten besluta i fall där åtgärden kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den hos vilken åtgärden vidtas (28 kap. 4 § första stycket RB). Ledning för vad som är stor omfattning respektive synnerlig olägenhet kan hämtas ur de uttalanden och den praxis som finns angående annan husrannsakan.

Utvidgning av husrannsakan

Om det under en påbörjad husrannsakan kommer fram uppgifter som ger anledning att tro att den eftersökta informationen lagras i ett annat datorsystem inom landet och uppgifterna är lagligen åtkomliga från det första systemet skall det, enligt artikel 19 punkt 2, vara möjligt att snabbt utvidga husrannsakan till att omfatta den information som finns i det andra systemet.

Om man först ser på frågan om det med nuvarande regler är möjligt att utvidga en pågående husrannsakan till att söka efter informationen någon annanstans är svaret i princip ja. Vad som dock måste beaktas är att beslutsfattaren måste kontaktas på nytt för att ta ställning i saken, om inte den som verkställer åtgärden själv är behörig att fatta beslut om husrannsakan i det utrymme som inte omfattas av det ursprungliga beslutet. Vidare måste – särskilt i de fall där det är fråga om husrannsakan hos annan – beslutsfattaren givetvis ta ställning till om de krav som ställs på en sådan husrannsakan är uppfyllda. Om beslutsfattaren utvidgar beslutet om husrannsakan – vilket kan ske efter en föredragning per telefon – kan åtgärden omedelbart verkställas.

[43] En förundersökningsledare inom Tullverket får genom hänvisningen i 19 § första stycket lagen om straff för smuggling motsvarande behörighet.

Saken kompliceras emellertid av att en sådan utvidgning som konventionen syftar på förutsätter att det finns möjlighet att verkställa husrannsakan ”på distans”. Den frågan behandlas i det följande.

Husrannsakan via elektroniska kommunikationsnät

Frågan om det är tillåtet att genomföra husrannsakan via elektroniska kommunikationsnät måste bedömas med utgångspunkt i utformningen av straffbestämmelsen om dataintrång. Att koppla upp sig mot någon annans dator i Sverige och ta del av information som finns lagrad där utgör dataintrång om det sker olovligen. I avsaknad av en lagregel som ger brottsbekämpande myndigheter rätt att med tvång vidta en sådan åtgärd torde det därför inte vara tillåtet att genomföra en husrannsakan via ett elektroniskt kommunikationsnät. Detta gäller även om en sådan åtgärd skulle vara skonsammare i det enskilda fallet.[44]

Om man vill göra det möjligt att verkställa husrannsakan på distans är det således nödvändigt att införa en särskild regel om detta. En sådan regel kan väl försvaras, eftersom det i många fall torde vara betydligt mindre ingripande att genomföra husrannsakan via ett kommunikationsnät än att genomföra den på plats. Särskilt i de fall husrannsakan riktar sig mot tredje man och äger rum med dennes samverkan kan det därför vara av värde att kunna använda sig av de tekniska möjligheter som finns för att genomföra åtgärden så snabbt och diskret som möjligt.

Samtidigt kan invändas att en möjlighet att verkställa husrannsakan via nät skapar större risker för missbruk, eftersom den som drabbas av husrannsakan då inte har samma möjligheter som annars att genom sin närvaro hindra övertramp. En sådan invändning kan emellertid bemötas genom att man ställer högre krav på beslut om husrannsakan via nät. Det skulle ligga i linje med regleringen av hemliga tvångsmedel om endast domstol ges behörighet att fatta beslut i sådana frågor. Om den som utsätts

[44] Datastraffrättsutredningen föreslog bl.a. av det skälet att husrannsakan i vissa fall skulle få verkställas via telenät, SOU 1992: 110 s. 363.

för åtgärden nämligen inte är närvarande där husrannsakan företas kan man med visst fog jämföra husrannsakan via nät med tvångsmedel som verkställs i hemlighet. Det torde också bli fråga om ett begränsat antal fall där frågan aktualiseras. Den extra tidsutdräkt som det innebär att inhämta beslut från domstolen får därför godtas, med tanke på den ökade rättssäkerhet som domstolsprövning innebär. Till dess att man har vunnit närmare erfarenheter bör därför endast domstol få besluta om husrannsakan via elektroniska kommunikationsnät. På sikt kan det finnas skäl att överväga om åklagare skall ha rätt att besluta om sådan husrannsakan.

Det finns dock en situation där åklagare redan nu bör ges rätten att besluta, nämligen om åtgärden genomförs med stöd av samtycke. Enligt doktrinen kan ett rättsligt bindande samtycke till en tvångsåtgärd endast avges till någon som är behörig att besluta om åtgärden (JO 1965 s. 163 och 1991/92 s. 116). Det är rimligt att anta att den som själv har utsatts för dataintrång, eller vars datautrustning har missbrukats på annat sätt, och som samtycker till husrannsakan, ser det som en fördel om denna kan verkställas via kommunikationsnät. I sådana fall bör åklagare kunna besluta om husrannsakan.

Frågan är om den föreslagna regleringen uppfyller kraven i artikel 19 punkt 2 på att en husrannsakan snabbt skall kunna utvidgas. I de fall åklagare kan besluta om husrannsakan förhåller det sig tveklöst så. Det torde även vara möjligt att tillräckligt snabbt kunna utverka ett domstolsbeslut i dessa fall. En husrannsakan som kräver medverkan av IT-experter är nämligen som regel väl planerad. I den planeringen bör även ingå frågan om det kan komma att krävas verkställighet via nät och om det därför krävs beslut av domstol.

I sammanhanget bör också beaktas möjligheten för åklagare att besluta om förbud mot att rubba bevisningen till dess att domstol har hunnit ta ställning.

Verkställigheten

I fråga om verkställighet av en vanlig husrannsakan i IT-miljö bör i princip samma regler gälla som för husrannsakan i allmänhet. Några särskilda regler om verkställigheten behövs därför inte.

För husrannsakan via elektroniska kommunikationsnät krävs däremot särskilda regler. Regeln i 28 kap. 6 § tredje stycket RB har tillkommit för att enskilda inte skall störas i onödan under den tid på dygnet när de normalt har sin nattvila. Något sådant undantag behövs inte för husrannsakan via nät. Likaså är bestämmelserna i 7 § anpassade för husrannsakan som verkställs i en fysisk miljö. De enda regler i 7 § som bör vara tillämpliga på husrannsakan via nät är bestämmelserna om rätt att anlita biträde av målsägande, sakkunnig eller annan, om målsägandens eller dennes ombuds rätt att närvara samt om underrättelse till den som har drabbats av åtgärden.[45]

Övriga frågor

En fråga som har tagits upp i det föregående är vilka möjligheter de brottsbekämpande myndigheterna har att ta del av information som normalt är tillgänglig för alla, t.ex. att besöka en webbsida, om den som tillhandahåller denna har ställt som villkor att poliser och andra brottsbekämpare inte får ta del av informationen. Så länge bestämmelsen om dataintrång straffbelägger varje form av olovligt intrång innebär detta en automatisk begränsning. Frågan är dock hur långt denna begränsning sträcker sig. Man kan nämligen fråga sig om det är rimligt att polisen har vidsträckta möjligheter att skaffa information inom ramen för sin spaningsverksamhet, t.ex. att fotografera personer eller att fysiskt följa efter dem, medan den inte får ta del av allmänt tillgängligt material på Internet till följd av att den som förfogar

[45] Beredningen för rättsväsendets utveckling har i betänkandet Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74) föreslagit viss ändring i 28 kap. 7 § RB. Det förslaget har inte beaktats i denna promemoria.

över en hemsida har förklarat polisen ”icke önskvärd”. En reglering som leder till det resultatet kan av polisen upplevas som orättfärdig och därmed inbjuda till kringgående, vilket självfallet är olyckligt.

IT-utredningen övervägde denna fråga. Utredningen ansåg att en överträdelse av ett villkor som förbjuder brottsbekämpande myndigheter tillträde till en elektronisk förmedlingstjänst inte innebär ett dataintrång. Utredningen grundade detta ställningstagande på att den som tillhandahåller en sådan tjänst inte kan förfoga över olovlighetsrekvisitet i straffbestämmelsen (SOU 1996:40 s. 210). Å andra sidan framhöll utredningen att det inte kunde accepteras att en polisman medvetet använder felaktiga identitetsuppgifter för att dölja vem han är. Utredningen hänvisade till de allmänna principer som riksdagen har lagt fast för vilka arbetsmetoder som får användas inom den öppna polisen (prop. 1983/84:111 s. 46 f). Frågan togs aldrig upp i propositionen. Någon rättspraxis som kan belysa frågan finns inte heller. Det är således alltjämt en tolkningsfråga hur långt polisen kan sträcka sig när det gäller att hämta in information av det slag som nu diskuteras.

I sammanhanget bör också nämnas att Beredningen för rättsväsendets utveckling nyligen har lagt fram förslag om rätt för polismän att uppträda under falsk identitet (SOU 2003:74 s. 179 ff). Utredningen föreslår även att polisen i ökad utsträckning skall få använda provokation som arbetsmetod, vilket bl.a. skulle innefatta en rätt att provocera fram brott (s. 141 ff). Betänkandet har remissbehandlats och är nu föremål för beredning

Så länge straffbestämmelsen om dataintrång förblir oförändrad i nu aktuella hänseenden och det råder delade meningar om hur olovlighetsrekvisitet skall tolkas finns det anledning att rekommendera försiktighet. Om man, som i vissa andra länder, inför en allmän reglering av polisens informationsinhämtande skulle frågan komma i ett annat läge. Detsamma gäller om nyss redovisade förslag om ändrade arbetsmetoder för polisen genomförs.

11.6.4 Anpassning av reglerna om beslag m.m.

Förslag: Ett förtydligande görs i den grundläggande regeln om beslag så att det framgår direkt av paragrafen att även elektroniska upptagningar kan tas i beslag. I fråga om elektroniska upptagningar av skrift skall gälla samma regler som för traditionella handlingar. Därmed görs det också klart att reglerna om beslagsförbud omfattar sådan bevisning i elektronisk form. Motsvarande ändringar görs i reglerna om editionsskyldighet och om skyldighet att tillhandahålla föremål för syn.

Som nyss har redovisats tar reglerna om beslag sikte på fysiska föremål, till vilka även skriftliga handlingar räknas. Det som faktiskt tas i beslag vid en husrannsakan i IT-miljö torde alltid uppfylla kravet på fysiskt föremål, vare sig det är fråga om en dator (eller någon del därav) eller en diskett, CD eller annan databärare eller en kopia eller en utskrift av en viss mängd datainformation. Utvecklingen har således visat att beslagsreglerna kan tillämpas även i en modern teknisk miljö. De behöver därför inte ändras av det skälet.

Däremot har det förhållandet att endast skriftlig handling nämns i den för beslagshanteringen centrala regeln om beslagsförbud (27 kap. 2 § RB) fått till följd att sådan information som lagras i elektronisk form och som rör uppgifter som omfattas av tystnadsplikt formellt har ett betydligt sämre skydd än motsvarande uppgifter i traditionella handlingar.

Även om användningen i rättegångsbalken av uttrycken skriftlig respektive handling inte generellt anses hindra en tolkning som innebär att både traditionella och elektroniska handlingar avses (se Ds 2003:29 s. 66), kan dessa begrepp sedda i sitt sammanhang hindra en sådan tolkning. Beslagsreglerna är ett exempel på detta, eftersom de förutsätter att det är fråga om en handling som samtidigt utgör ett föremål. Visserligen kan hävdas att regeln om beslagsförbud dels kan vara analogt tillämplig på informationen i dess elektroniska form, dels att den blir tillämplig så snart den elektroniska informationen materialiseras i form av

en traditionell handling. Skadan i form av informationsintrånget har emellertid då redan skett. Eftersom det är tillåtet att fritt använda överskottsinformation kan intrånget därför få konsekvenser för den enskilde, även om det vid en senare tidpunkt konstateras att reglerna i 27 kap. 2 § RB hindrar beslag.[46] Så länge informationen är kvar i elektronisk form torde det inte vara möjligt att ingripa mot en tjänsteman som hanterar den i strid med bestämmelserna i 27 kap. 2 § RB, trots att Högsta domstolen har framhållit att den regeln vid tveksamhet skall tolkas till den enskildes förmån (NJA 1977 s. 403).

Konventionen innebär ett förpliktigande att se till att de processrättsliga reglerna uppfyller tillräckliga rättssäkerhetsgarantier (artiklarna 14 och 15). En av de viktigaste rättssäkerhetsgarantierna i den nuvarande regleringen av beslag, beslagsförbuden, har till följd av den ökade datoriseringen kommit att urholkas på ett sätt som varken har varit avsett av lagstiftaren eller som kan anses godtagbart.

Bestämmelsen i 27 kap. 1 § RB bör därför förtydligas, för att markera att inte bara handlingar utan även elektroniska upptagningar kan bli föremål för beslag. Avsikten med ändringen är enbart att anpassa rättegångsbalkens beslagsregler till ny teknik, inte att utvidga tillämpningsområdet.

Vidare bör det direkt av paragrafen framgå att särbestämmelserna om skriftlig handling skall tillämpas på elektroniska upptagningar av skrift. Därmed finns det inte längre någon tvekan om att beslagsförbuden träffar samma typ av information i elektronisk form som återfinns i traditionella handlingar. Det innebär också att reglerna om skyndsam granskning och om vem som får granska materialet blir direkt tillämpliga på bevisning i elektronisk form.

En motsvarande begränsning till skriftlig handling finns i flera andra bestämmelser i rättegångsbalken, bl.a. i 38 kap. 2 §, som reglerar vad som kan blir föremål för edition, och i 39 kap. 5 §, som reglerar skyldigheten att tillhandahålla föremål för syn.

[46] Det förslag till reglering av överskottsinformation som har presenterats i Ds 2003:13 ändrar inte detta förhållande.

Även om det, till följd av Högsta domstolens ställningstagande i NJA 1998 s. 829, kan hävdas att reglerna om edition numera kan tillämpas även på information i elektronisk form som inte har materialiserats bör ändå nu nämnda bestämmelser förtydligas på motsvarande sätt. Dessa kan nämligen komma att tillämpas i situationer som omfattas av konventionens tillämpningsområde, t.ex. vid intrång i upphovsrätt.

Däremot föreslås inga ändringar i andra bestämmelser i rättegångsbalken där uttrycket skriftlig handling förekommer.

11.6.5 Kopiering av bevis

Bedömning: Det är inte nödvändigt att införa nya regler om kopiering av bevis i elektronisk form för att anpassa den svenska lagstiftningen till konventionen. Frågan om kopiering har dock stor principiell och praktisk betydelse och bör därför ses över, men detta kräver ett vidare perspektiv än vad detta ärende erbjuder.

Allmän bakgrund

Enligt artikel 19 punkt 3 skall det vara möjligt för de brottsbekämpande myndigheterna att göra och behålla en kopia av datorbehandlingsbara uppgifter som säkras genom husrannsakan, beslag eller annat liknande förfarande. Detta aktualiserar den omdiskuterade frågan om, och i så fall i vilken utsträckning, myndigheter har rätt att kopiera information som tas i beslag och hur man senare skall förfara med sådana kopior.

Det finns inte några generella regler i svensk rätt om hur polisen och andra brottsbekämpande myndigheter får hämta in och använda information i en brottsutredning. Detta skall ses mot bakgrund av att det är tillåtet att anföra all slags bevisning i ett brottmål och den grundläggande principen om domstolens fria bevisprövning. Det finns inte heller något allmänt skydd mot att de brottsbekämpande myndigheterna genom avskrift, fotografe-

ring, kopiering eller annat tekniskt förfarande tillgodogör sig innehållet i handlingar som har tagits i beslag. Ofta är det nämligen innehållet i handlingen och inte handlingen som sådan som är av intresse för brottsutredningen. Regeln i 27 kap. 1 § andra stycket RB har, som tidigare nämnts, tillkommit för att möjliggöra beslag i dessa fall.

Det är vanligt att en originalhandling som har tagits i beslag fotokopieras eller kopieras på annat sätt. Kopieringen kan ha olika syften. Ett vanligt syfte är att begränsa intrånget för den som har drabbats av beslaget. Metoden med kopiering innebär i dessa fall att beslaget kan hävas tidigare än vad som annars hade varit möjligt. Ett annat syfte kan vara att framställa arbetsexemplar som kan användas t.ex. i samband med förhör. Tanken är att skona originalhandlingarna från förslitning, nedsmutsning och liknande försämring (jfr 27 kap. 10 § tredje stycket RB om vård av beslag). Detta kan vara aktuellt inte bara när originalhandlingen har ett ekonomiskt värde (t.ex. värdepapper eller kulturhistoriskt värdefulla dokument) utan även i andra fall.

Kopiering används också för att framställa kompletta exemplar av förundersökningsprotokollet. I stället för att åklagaren inför domstolen företer ett originalexemplar av den bevisning som åberopas i målet kopieras allt relevant material och tillförs varje exemplar av förundersökningsprotokollet. Den metoden torde vara en förutsättning för att man över huvud taget skall kunna genomföra rättegången exempelvis i omfattande mål om ekonomisk brottslighet, där normalt ett stort antal handlingar i form av exempelvis bolagshandlingar, avtal, bokföringshandlingar, korrespondens, deklarationer och liknande åberopas som bevisning. I dessa fall fyller kopieringen det syftet att såväl rätten som åklagaren samt alla tilltalade och deras försvarare på ett enkelt sätt får tillgång till samma skriftliga material.

Det förekommer även att en handling som normalt skulle ha tagits i beslag i stället enbart kopieras. Om kopieringen görs utan något beslut om beslag kan saken inte komma under domstols-

prövning. Något beslag har då inte ägt rum och det finns ingen laglig möjlighet att få förfarandet prövat.[47]

Kopiering och hantering av beslagtagna handlingar

Den numera mycket omfattande kopieringen av beslag är inte något som är förutsett i RB. Förfaringssättet med kopiering torde dock vara allmänt accepterat så länge åtgärden grundas på medgivande av eller önskemål från den som har drabbats av beslaget.

Det förhåller sig emellertid annorlunda om den som har drabbats av beslaget av något skäl motsätter sig beslaget eller att det beslagtagna kopieras. Förfarandet att kopiera och därefter häva beslag har nämligen den nackdelen att beslagsfrågan normalt inte kan prövas när beslaget har hävts (NJA 1977 s. 573 och 1990 s. 537). I undantagsfall kan dock en prövning ske trots att beslaget har hävts, nämligen om beslagsfrågan har betydelse i något annat rättsligt hänseende, t.ex. för rättegångskostnaderna eller för internationell rättslig hjälp (se NJA 1988 s. 86 och 471).

Från tid till annan har metoden med kopiering ifrågasatts (se bl.a. TSA 1978 s. 95, JK 1983 s. 195, JO 1982/83 s. 51 ff och NJA 1988 s. 471). Frågan har också utretts vid olika tillfällen.

Tvångsmedelskommittén föreslog att det skulle införas en rätt att få en beslagsfråga prövad även i fall där beslaget hade hävts, om någon uppgift som härrörde från beslaget fanns kvar hos den myndighet som hade gjort beslaget eller om denna hade överlämnat en sådan uppgift till någon annan myndighet. Prövningen skulle avse frågan om det funnits skäl för beslaget (SOU 1984:54 s. 207). I propositionen avvisade departementschefen förslaget (prop. 1988/89:124 s. 32).

Polisrättsutredningen konstaterade att metoden att kopiera handlingar och att därefter häva beslaget används ofta. Ett sådant förfarande kan enligt utredningen inte anses väl förenligt med grunderna för bestämmelsen om rätt att begära domstolspröv-

[47] Här bortses från möjligheten att indirekt få en prövning av förfarandet genom att anmäla befattningshavaren för tjänstefel eller förseelse i tjänsten.

ning av beslag, om det inte grundas på önskemål från eller medgivande av den som drabbats av beslaget (SOU 1995:47 s. 414). Utredningen fann dock att förfarandet trots detta måste godtas, eftersom rättens prövning ändå inte kan resultera i att de brottsutredande myndigheterna förbjuds att använda informationen. Utredningen lade inte fram något förslag med anknytning till frågan om kopiering (s. 197 ff).

Det är emellertid inte bara frågorna om det är tillåtet att använda kopiering och hur kopior får användas som har varit föremål för diskussion. Även frågan om de kopierade handlingarnas status och hur de skall hanteras när kopiorna inte längre fyller någon funktion har diskuterats.

En sådan fråga är om en beslagtagen handling alltid blir en allmän handling, oavsett syftet med beslaget och oberoende av om beslaget hävs. Ett skäl till att den frågan har kommit upp är ett uttalande i Polisrättsutredningens slutbetänkande (se SOU 1995:47 s. 200). Utredningen utgick nämligen från att reglerna i 2 kap. TF skall tillämpas på beslagtagna handlingar och att en beslagtagen handling skall behandlas som vilken inkommen handling som helst, utan något resonemang om vad detta synsätt leder till i praktiken. Utredningens synsätt grundades på att det i TF inte finns något uttryckligt undantag för beslagtagna handlingar. Frågan har inte belysts av lagstiftaren, eftersom utredningens betänkande inte har lett till någon åtgärd.

Vid en bokstavlig tolkning av reglerna i TF har utredningens resonemang onekligen fog för sig. Det finns nämligen inget undantag för beslagtagna handlingar. Å andra sidan finns det inte heller något uttalande vare sig i förarbetena till rättegångsbalken eller till TF som tyder på att en sådan tolkning har varit avsedd.

Beslag drabbar inte bara den som är misstänkt utan i stor utsträckning även brottsoffer och helt utomstående. Rättegångsbalkens regler utgår från att beslag är en tillfällig besittningsrubbning som skall återställas så snart som möjligt. I balken finns särskilda regler för hur beslag skall dokumenteras och vårdas samt för när beslaget skall upphöra. Det vanligaste syftet med beslag av handlingar är att få fram bevisning. Syftet kan

emellertid även vara att få tillgång till en handling som skall förverkas eller återlämnas till rätt ägare. Om handlingen skall förverkas eller återställas skulle det direkt motverka syftet med åtgärden om den beslagtagna handlingen skulle betraktas som allmän (och därmed vara underkastad de för allmänna handlingar gällande reglerna om registrering och bevarande).[48] Även när det gäller beslag i bevissyfte kan utredningens synsätt ifrågasättas. Om den beslagtagna handlingen (eller en kopia av den) tillförs förundersökningsprotokollet ingår den i en upprättad allmän handling. För protokollet gäller vanliga regler om allmänna handlingar. Det spelar då ingen roll om handlingen utgör ett original eller en kopia. Om handlingen emellertid inte behövs som bevisning skall den återställas i samband med att beslaget hävs.

Om man ser till syftet med offentlighetsprincipen, att ge allmänheten insyn i offentlig verksamhet, framstår uppfattningen att beslagtagna handlingar blir allmänna handlingar i och med beslaget som direkt irrationell. En beslagtagen handling torde inte ge någon inblick i myndigheternas verksamhet utan enbart i den enskildes personliga eller ekonomiska angelägenheter.

I den praktiska hanteringen torde inte beslagtagna handlingar behandlas som allmänna handlingar, utom i de fall där originalet eller en kopia tillförs en upprättad handling som i sig utgör en allmän handling. Det är emellertid allt vanligare att misstänkta och deras försvarare försöker kringgå reglerna i rättegångsbalken om rätt till insyn i förundersökningsmaterialet genom att begära att få del av beslagtagna handlingar med stöd av TF. Vid en sådan begäran måste givetvis frågan om den beslagtagna handlingen är att anse som allmän prövas.

Starka argument av såväl principiell som praktisk natur kan således anföras mot Polisrättsutredningens synsätt och de konsekvenser detta kan få för den som drabbas av beslag. Dess uttalanden har också lett till ökad osäkerhet om hanteringen av beslagtagna handlingar och kopior av sådana handlingar.

[48] Polisrättsutredningen såg, i konsekvens med sin uppfattning om att beslagtagna handlingar utgör allmänna handlingar, regeln om hävande av beslag som en gallringsregel.

Kopiering av information i elektronisk form

Frågan om kopiering har stor praktisk betydelse för hanteringen av bevisning i elektronisk form. Dagens datorer har nämligen så stor lagringskapacitet att det i de flesta fall är omöjligt att vid en husrannsakan på plats gå igenom all information i en dator. Av det skälet tas datorn ofta i beslag.

Eftersom datorstödet numera utgör en viktig förutsättning för verksamheten både för företag, myndigheter och enskilda har det stor betydelse om och i så fall hur lång tid de brottsbekämpande myndigheterna beslagtar hela eller centrala delar av datautrustningen (t.ex. en server). Mot den bakgrunden har JK framhållit att kopiering alltid bör övervägas som ett alternativ till beslag i dessa fall (JK:s beslut den 17 maj 2001, dnr 2806-00-21). JK konstaterade i beslutet att frågan om lagreglering av möjligheterna till kopiering kan behöva övervägas på nytt. Han överlämnade därför en kopia av beslutet till Justitiedepartementet.

Valet mellan beslag av databäraren och kopiering av den information som finns lagrad i denna är emellertid inte självklart, om man betraktar den teknik som ofta används för kopieringen.

För att bevara datainformationen i det skick den var när myndigheterna ingrep med tvångsmedel används ofta tekniken att spegla en beslagtagen dators innehåll på en annan hårddisk. Speglingstekniken innebär att en exakt, icke ändringsbar, kopia av hela innehållet görs. Ibland hävs beslaget avseende datorn eller delarna av datorsystemet när speglingen har genomförts. I andra fall får beslaget bestå. Det är således inte givet att spegling innebär att beslaget kan hävas snabbare än vad som annars varit fallet.

Ett viktigt skäl till att man använder speglade kopior är att undvika de felkällor som ligger i att filer ändras så snart någon öppnar dem. En ytlig undersökning av innehållet, även om det bara är fråga om att öppna ett dokument och läsa rubriken, kan därför inte skiljas från ingrepp och ändringar i själva dokumentet. Detta skapar utrymme för diskussion om informationsinnehållet har undergått förändringar under den tid som det har disponerats i en brottsutredning. Genom speglingstekniken kan påståenden om att de brottsbekämpande myndigheterna har ma-

nipulerat innehållet undvikas. Vidare kan datalagrad information gå förlorad redan genom att ett datasystem startas upp. Spegling är ett sätt att undvika det. Ett annat skäl till att spegling används är behovet av att söka efter raderad information. Det är inte möjligt att återskapa raderad information eller att undersöka vad som har raderats vid vanlig kopiering. I brottsutredningar kan kunskap om vad som har raderats och återskapande av raderad information spela stor roll. Ett tredje skäl som anförs för användningen av spegling är att polisen undviker att installera och använda sina analysprogram i en främmande datamiljö, med de risker för bl.a. skador som det kan innebära.

Speglingstekniken skapar emellertid också problem. Om det nämligen visar sig att någon del av materialet inte får tas i beslag, eller att det inte längre finns grund för beslaget i viss del, är det inte tekniskt möjligt att skilja ut detta från den speglade kopian. Det står inte i överensstämmelse vare sig med den nuvarande lagstiftningen (27 kap. 8 § första stycket RB) eller med lagstiftarens intentioner att på detta sätt behålla beslag enbart av tekniska skäl. Tekniken innebär dessutom att det oundvikligen skapas stora mängder av överskottsinformation. Ett utvidgat internationellt samarbete sätter fokus på användningen av denna teknik. Det är därför angeläget att frågan om en rättsenlig användning av speglingstekniken löses.

Till dess frågan om att skilja ut information som inte längre skall vara i beslag har lösts bör speglingstekniken därför inte användas rutinmässigt utan bara i de fall där det finns särskild anledning att anta att hanteringen av informationen kan komma att ifrågasättas, eller där det annars kan anföras särskilda skäl för att just denna teknik bör väljas trots integritetsintrånget. Vid utredning av dataintrång, brytande av telehemlighet och vissa andra datorrelaterade brott torde det normalt finnas starkare skäl att utnyttja speglingstekniken än vid utredning av t.ex. förmögenhetsbrott. Om det finns starka skäl att tro att information som är av betydelse i utredningen har raderats kan detta vara ett särskilt skäl för att använda spegling.

Något som också bör vägas in vid bedömningen av om speglingsteknik skall användas är sannolikheten för att något som inte får tas i beslag enligt 27 kap. 2 § RB påträffas. I vissa fall är det osannolikt att det finns sådan information (t.ex. om bokföring tas i beslag hos en från den misstänkte fristående bokförare) medan det i andra fall är högst sannolikt (t.ex. om det är fråga om beslag hos någon som tillhör någon av de yrkeskategorier som anges i 36 kap. 5 § RB). Ju större risken är för att en spegling kan komma att omfatta något som inte får tas i beslag, desto starkare är skälen emot att använda spegling.

Vad som nu har sagts gäller spegling av hela innehållet i en dator. Spegling kan i och för sig begränsas till enbart en viss del av den lagrade informationen. Även vid en partiell spegling uppstår de problem som har beskrivits ovan, såvitt gäller den speglade informationen.

I de fall där spegling inte är oundgänglig bör vanlig kopiering av datainformation användas. Det är dessutom långtifrån alltid nödvändigt att ta del av den samlade informationen i en hårddisk. I vissa fall står det redan från början klart att det som eftersöks är ett visst dokument, en viss fil eller någon annan identifierbar enhet av den samlade informationen. Undersökningen kan då ofta begränsas. Informationen kan kopieras och överföras t.ex. till diskett eller CD.

Frågan om kopiering av information i elektronisk form aktualiseras också i de fall där det i samband med husrannsakan och beslag tas utskrifter av enstaka handlingar. Eftersom det i datormiljö normalt inte kan göras någon skillnad mellan originalhandlingar och kopior kan det diskuteras om en sådan utskrift har status som kopia eller ej.

Överskottsinformation

Frågan om tillåtligheten av kopiering har ett nära samband med frågan om användning av s.k. överskottsinformation. Med överskottsinformation avses normalt sådan information om brott som har kommit till polisens kännedom genom använd-

ning av tvångsmedel vid utredning av ett helt annat brott. Som framgått av vad som har sagts ovan om spegling kan själva kopieringstekniken innebära att stora mängder överskottsinformation skapas. För närvarande får överskottsinformation användas utan några begränsningar (prop. 1988/89:124 s. 29 ff).

Kopiering av relevant material är ett enkelt och praktiskt sätt att möjliggöra användning av överskottsinformation. Kopiering har också den fördelen att informationen överförs i exakt den form som den hade när den kom till brottsbekämpande myndigheters kännedom. Överskottsinformation som har kopierats kan läggas till grund för en ny förundersökning, användas som underlag för underrättelseverksamhet eller nyttiggöras på annat sätt i polisens verksamhet, t.ex. som underlag för det brottsförebyggande arbetet.

När regeringen senast tog ställning till frågan om reglering av användning av överskottsinformation framhöll den att frågan om hur kopierat material skall få användas är något som lämpar sig mindre väl för lagreglering (a. prop. s 32).

Frågan om användning av överskottsinformation har nyligen utretts på nytt. En promemoria med förslag till reglering av sådan överskottsinformation som härrör från användning av hemliga tvångsmedel har presenterats (Ds 2003:13). Användning av annan överskottsinformation föreslås förbli oreglerad. Användningen av kopior av beslagtaget material berörs således inte av förslaget. Promemorian har remissbehandlats. Regeringen har ännu inte tagit ställning till förslagen i promemorian.

Slutsatser

Frågan om kopiering inrymmer flera olika problem. Man måste skilja mellan å ena sidan det fallet att något kopieras i stället för att det tas i beslag och å andra sidan det fallet att något som med laga stöd har tagits i beslag kopieras. I det förra fallet är det tveksamt om förfaringssättet alls står i överensstämmelse med regelsystemet i RB om det sker mot den drabbades vilja, eftersom denne då sätts ur stånd att få åtgärden domstolsprövad. Den frå-

gan saknar emellertid intresse här. I det senare fallet finns det lagstöd för beslag, medan den fortsatta hanteringen är oreglerad.

Det torde vara oundvikligt att sådant material som tagits i beslag kopieras som ett led i brottsutredningen och föreberedelserna för rättegången. Detta gäller såväl skriftliga handlingar som annat som det är möjligt att kopiera. Det är inte heller själva kopieringen som de flesta har vänt sig mot, utan mot att det inte finns några begränsningar av användningen och inte heller några andra regler som styr den fortsatta hanteringen av kopiorna i de fall där beslaget hävs. Kritikerna (bl.a. JK) har därför ansett att det är tveksamt om metoden med kopiering av handlingar bör få användas i de fall där ett beslag har gjorts och detta sedermera hävs. De har förordat att, om metoden används, beslaget i varje fall inte bör hävas innan den drabbade har haft möjlighet att föra saken till domstolsprövning. Å andra sidan har JK i ett senare beslut framhållit fördelarna med kopiering som alternativ till beslag av datorutrustning. JO har framhållit att kopiering har både fördelar och nackdelar och allmänt sett varit mera positiv till förfarandet än JK. Riksåklagaren har förfäktat att förfarandet är nödvändigt och att det inte medför några större risker för den enskilde.

Motsvarande synpunkter torde kunna anläggas i fråga om kopiering av bevis i elektronisk form, även om den frågan hittills inte har väckt samma uppmärksamhet.

Behovet av kopiering torde vara särskilt stort när det är fråga om material som beslagtas som ett led i utredningar om IT-relaterade brott. Ett huvudskäl till detta är att datainformation är flyktig i den meningen att den snabbt kan förändras och att det kan vara svårt att i efterhand återskapa den information som har funnits vid en given tidpunkt. Av det skälet är det viktigt att kunna genom kopiering eller på annat sätt frysa situationen så att den relevanta informationen behålls oförändrad. Ett annat skäl till att kopiering spelar en särskilt viktig roll vid utredning av IT-relaterade brott är att beslag av datorer och annan datautrustning kan komma att stå i strid med proportionalitetsprincipen, om det leder till att den som drabbas av beslaget över huvud taget inte

kan använda sin datorutrustning under den tid som beslaget varar.

Den nuvarande lagstiftningen lägger emellertid inga formella hinder i vägen när det gäller möjligheterna att kopiera material i en förundersökning. Anpassningen till konventionen kan därför inte sägas göra det absolut nödvändigt att införa regler om kopiering av bevis i elektronisk form. Skulle användningen av överskottsinformation lagregleras kan saken emellertid komma i ett annat läge. En generell reglering av överskottsinformation skulle träffa kopiering av alla typer av bevisning i elektronisk form, medan en reglering i linje med vad som har föreslagits i den tidigare nämnda promemorian om överskottsinformation enbart har intresse för sådan bevisning som härrör från hemliga tvångsmedel.

Det är uppenbart att frågan om kopiering har många olika både principiella och praktiska aspekter och därför måste ses ur ett betydligt bredare perspektiv än vad detta arbete medger. Den lämpar sig även av det skälet inte för lagstiftning i detta sammanhang. Några förslag om regler för kopiering av beslag läggs därför inte fram. Det finns emellertid goda skäl att överväga frågan i annat sammanhang.

11.7 Telenät av mindre betydelse

Förslag: Tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning utvidgas något genom att undantaget för avlyssning av kommunikationsnät av begränsad betydelse från allmän kommunikationssynpunkt görs snävare. Endast kommunikationsnät som saknar betydelse från allmän kommunikationssynpunkt bör undantas.

Genom en lagändring som trädde i kraft år 1996 gjordes reglerna om hemlig teleavlyssning och hemlig teleövervakning tillämpliga på alla telenät oavsett i vilken regi de drivs. Ändringen föranleddes av den öppna telemarknaden, vilken innebar att rätten att

bedriva televerksamhet hade gått över från ett statligt organ till bolag.

För att inte bestämmelserna om tvångsmedel skulle bli alltför vittomfattande och gälla för kommunikationsnät som sällan eller aldrig har betydelse från brottsutredningssynpunkt infördes en generell begränsning. Den innebär att hemlig teleavlyssning och hemlig teleövervakning inte får förekomma inom telenät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt. Med detta åsyftas bl.a. intern telekommunikation i och intill en bostad t.ex. via snabbtelefoner, PC-nät och liknande utrustning, hörselslingor för hörselskadade och interna system för personsökning i form av fasta installationer (prop. 1994/95:227 s. 27). Däremot undantas inte sådana telenät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga telenät och inte heller större företagsnät. Fristående datorer som är försedda med modem och datorer i små interna nätverk som via andra nätverk kommunicerar med varandra eller med elektroniska anslagstavlor, databaser eller andra informationssystem kan också bli föremål för hemlig teleavlyssning och hemlig teleövervakning (a. prop. s. 31). Om telekommunikationen endast äger rum internt inom ett slutet nät bör det enligt förarbetena krävas att nätet är av större omfattning för att en tvångsåtgärd skall få äga rum. Det är emellertid inte bara antalet anslutningar och den geografiska spridningen som är avgörande. Frågan om ett telenät skall anses vara av mindre betydelse skall enligt förarbetena prövas utifrån en samlad bedömning av samtliga omständigheter.

Det finns inga rättsfall som belyser frågan om vilka kommunikationsnät som faller utanför tillämpningsområdet för hemlig teleavlyssning eller hemlig teleövervakning. Det är därför osäkert hur långt det nuvarande undantaget sträcker sig.

I konventionen görs inte något undantag för kommunikationsnät av mindre betydelse. Däremot finns enligt artikel 14 punkt 3 b möjlighet för staterna att utfärda förbehåll, om det i befintlig lagstiftning finns begränsningar som innebär att avlyss-

ning respektive inhämtande av trafikuppgifter i realtid inte får tillämpas på en tjänsteleverantörs system som drivs för en sluten användargrupp och som inte använder allmänna kommunikationsnät samt inte är kopplat till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

Det aktualiserar frågan om det nuvarande undantaget för telenät som är av mindre betydelse från allmän kommunikationssynpunkt står i överensstämmelse med konventionens krav. Så som undantaget har beskrivits i förarbetena torde det omfatta fler användare än vad möjligheten till förbehåll i konventionen medger. Eftersom det är fråga om ett undantag ligger det i sakens natur att frågan om undantagets gränser sällan kan komma under domstolsprövning.

Sett ur integritetssynpunkt har det nuvarande undantaget främst betydelse för användningen av avlyssning. Det man har velat undanta är sådana enskilda kommunikationsnät som kan sägas vara betydelselösa för brottsbekämpningen men där det skulle innebära ett avsevärt integritetsintrång med avlyssning. Att undantaget även gäller för hemlig teleövervakning är mera svårförståeligt, eftersom de uppgifter som det tvångsmedlet resulterar i rör vilken extern kommunikation som har förekommit. Mot den bakgrunden kan man ifrågasätta om det över huvud taget behövs något undantag för nät av mindre betydelse vid hemlig teleövervakning.

Det nuvarande undantaget för nät av mindre betydelse från kommunikationssynpunkt måste göras snävare för att Sverige skall uppfylla åtagandena i konventionen. En möjlighet kan vara att helt avskaffa det i fråga om hemlig teleövervakning. Mot den lösningen talar dock att hemlig teleavlyssning och hemlig teleövervakning oftast används parallellt och att det har betydande fördelar att använda samma definitioner och grundläggande regler för båda tvångsmedlen. En lämplig lösning kan i stället vara att enbart undanta sådana nät som saknar betydelse från allmän kommunikationssynpunkt. För att ett nät skall anses sakna betydelse bör krävas dels att det är fråga om ett slutet nät som inte är kopplat till något allmänt kommunikationsnät, dels att det

inte heller i övrigt är sammankopplat med eller kan kommunicera med annat nät. Det innebär att bl.a. porttelefoner, snabbtelefoner, system för intern personsökning och hörselslingor alltjämt kommer att falla utanför tillämpningsområdet. Detsamma kommer att gälla enstaka datorer som inte är uppkopplade mot något kommunikationsnät.

Det bör anmärkas att den praktiska betydelsen av ändringen är begränsad. Den som ansvarar för ett privat kommunikationsnät har nämligen inte de skyldigheter som åvilar den som tillhandahåller ett allmänt kommunikationsnät att bistå brottsbekämpande myndigheter.

När paragrafen ändras bör samtidigt uttrycket telenät bytas ut mot det uttryck som används numera, nämligen det teknikneutrala kommunikationsnät.

11.8 Frågor om sekretess och tystnadsplikt m.m.

11.8.1 Sekretess i det allmännas verksamhet m.m.

Förslag: De nuvarande sekretessreglerna till skydd för såväl brottsutredande verksamhet som enskildas personliga och ekonomiska förhållanden är så generellt utformade att det inte krävs någon ändring i dessa, om nya tvångsmedel införs. Däremot krävs det en uttrycklig regel om att uppgifter om frysning av elektronisk kommunikation och kvarhållande av elektronisk post – i likhet med vad som gäller för användning av andra hemliga tvångsmedel – skall undantas från meddelarfriheten. Ändringar med denna innebörd föreslås i 16 kap. 1 § sekretesslagen.

Kraven i konventionen på regler om sekretess hos och informationsutbyte mellan myndigheter är, som tidigare nämnts, redan uppfyllda genom de nuvarande sekretessreglerna (se avsnitt 6.5).

Införandet av nya tvångsmedel väcker emellertid frågan om den nuvarande sekretessregleringen behöver kompletteras i något hänseende. Sekretesskyddet i 5 kap. 1 och 7 §§ (sekretess till

skydd för den brottsbeivrande verksamheten) och i 9 kap. 17 § sekretesslagen (sekretess till skydd för enskilds personliga eller ekonomiska förhållanden) är så generellt utformat att det inte behövs några kompletterande sekretessbestämmelser för nya tvångsmedel. Vad som däremot bör övervägas är huruvida det bör råda meddelarfrihet eller inte för uppgifter som hänför sig till användning av de nya tvångsmedlen.

Det råder enligt 16 kap. 1 § sekretesslagen meddelarfrihet för alla uppgifter som skyddas av sekretess till förmån för enskilds personliga eller ekonomiska förhållanden i en brottsutredning. Det råder även meddelarfrihet för de allra flesta uppgifter som omfattas av sekretess till skydd för den brottsbeivrande verksamheten, även uppgifter om användning av tvångsmedel. Det enda undantaget från meddelarfriheten är användning av hemliga tvångsmedel. För uppgifter som omfattas av sekretess enligt 5 kap. 1 § sekretesslagen och som avser användning av hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning och kvarhållande av försändelse gäller inte meddelarfrihet. Motsvarande begränsning finns för uppgifter om användning av hemliga tvångsmedel som är sekretesskyddade genom regeln i 5 kap. 7 §.

Frysning av elektronisk kommunikation är ett förstadium till hemlig teleavlyssning och hemlig teleövervakning. Samma skäl som talar för att det krävs undantag från meddelarfriheten beträffande dessa tvångsmedel gör sig gällande beträffande frysning. Frysning av elektronisk kommunikation bör således undantas från meddelarfriheten genom att ett tillägg görs i 16 kap. 1 § sekretesslagen.

På motsvarande sätt bör uppgifter om kvarhållande av elektronisk post undantas från meddelarfriheten, i likhet med vad som är fallet med kvarhållande av traditionell post.

Frågan om den automatiserade behandling av personuppgifter som äger rum vid hemlig teleavlyssning och hemlig teleövervakning bör falla under polisdatalagen besvarades nekande vid lagens tillkomst. På den efterföljande bearbetningen och lagringen tillämpas dock polisdatalagen (SOU 1997:65 s. 197 f). Samma

ståndpunkt har intagits av Polisdatautredningen i betänkandet Behandling av personuppgifter i polisens verksamhet (SOU 2001:92 s. 159 f). Det är således uteslutande reglerna i RB som styr hur uppgifterna får användas. Detsamma kommer automatiskt att gälla för uppgifter som har varit föremål för frysning. Om Polisdatautredningens förslag genomförs kan det därför bli aktuellt med en ändring i den föreslagna 1 kap. 3 § polisdatalagen. Eftersom frågan om ändringar i lagstiftningen om polisens dataregister fortfarande är föremål för beredning i regeringskansliet läggs inte någon sådant förslag fram här.

11.8.2 Sekretess hos operatörer

Förslag: Operatörers tystnadsplikt skall omfatta även frysning av elektronisk kommunikation. En regel om detta införs i lagen om elektronisk kommunikation. Deras tystnadsplikt omfattar redan i dag kvarhållande av traditionella försändelser, men bör även omfatta kvarhållande av elektronisk post.

Beslut om hemliga tvångsmedel på teleområdet verkställs av operatörerna på uppdrag av polisen. Operatörerna, som är privata rättssubjekt, omfattas inte av reglerna i sekretesslagen. Dessa har i stället ålagts tystnadsplikt avseende användningen av hemliga tvångsmedel genom en regel i lagen om elektronisk kommunikation (6 kap. 21 §). Regeln har i sak oförändrad förts över från telelagen.

Av samma skäl som det krävs en regel om tystnadsplikt för operatörer för verkställighet av hemlig teleavlyssning och hemlig teleövervakning krävs det en uttrycklig reglering av tystnadsplikten om frysning av elektronisk kommunikation införs som nytt tvångsmedel. Om Sverige skall uppfylla sina åtaganden enligt konventionen (artiklarna 16, 20 och 21) bör därför ett tillägg göras i 6 kap. 21 § lagen om elektronisk kommunikation, så att operatörernas tystnadsplikt omfattar även frysning.

Det finns redan en regel om tystnadsplikt för operatörer som avser åtgärden att kvarhålla försändelser enligt 27 kap. 9 § RB. Man kan ifrågasätta vilken funktion denna regel har med dagens lagstiftning, eftersom begreppet försändelse i 27 kap. 3 och 9 §§ RB avser ett fysiskt föremål i form av ett brev, paket eller liknande. Regeln i fråga infördes när telelagen kom till. Förarbetena ger ingen förklaring till varför lagen kom att innehålla en tystnadspliktsregel som i första hand tar sikte på postbefordran, men en sannolik förklaring är att det är en kvarleva från den tid då telegram var ett vanligt kommunikationssätt. Regeln fördes i oförändrat skick över till lagen om elektronisk kommunikation.

Om reglerna om kvarhållande av traditionell post och av elektronisk post placeras i samma paragraf behövs inte någon utvidgning av tystnadsplikten. Nu har i stället valts en lösning med två olika paragrafer för kvarhållande av post. Det aktualiserar frågan om den nuvarande tystnadsplikten behöver utvidgas. För tydlighetens skull bör det direkt framgå att tystnadsplikten omfattar angelägenheter som rör kvarhållande av elektronisk post.

11.8.3 Trafikuppgifter, abonnemangsuppgifter och lokaliseringsuppgifter

Förslag: En operatör skall på begäran röja trafikuppgifter beträffande ett särskilt utpekat telemeddelande, om uppgifterna behövs för att spåra den väg på vilken meddelandet överfördes och vilken eller vilka tjänsteleverantörer som medverkat i överföringen. Polisen och åklagare kan begära att få ut sådana trafikuppgifter, vilka får röjas endast om det är föreskrivet fängelse ett år för brottet. En regel om detta införs i lagen om elektronisk kommunikation. Bestämmelsen utformas efter mönster av lagens övriga regler om utlämnande av uppgifter för vilka tystnadsplikt gäller.

Trafikuppgifter

Trafikuppgift definieras i 6 kap. 1 § lagen om elektronisk kommunikation som en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. I konventionen definieras trafikuppgift som sådana uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av datorer, som skapas av ett datorsystem som ingår i kommunikationskedjan och som anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst. Det finns ingen saklig skillnad mellan definitionerna.

Inom EU pågår för närvarande diskussioner om man bör ändra de regler som styr operatörernas skyldighet att bevara trafikuppgifter. Som tidigare har nämnts är för närvarande huvudprincipen att sådana uppgifter av integritetsskäl endast får bevaras en kort tid. Som ett led i en effektivare brottsbekämpning (bl.a. bekämpning av terrorism) pågår arbete med utkast till ett rambeslut om bevarande av uppgifter relaterade till Internet- och telefontrafik. Huvudsyftet med rambeslutet är att skapa bättre förutsättningar för de brottsbekämpande myndigheterna att utreda allvarlig brottslighet. Detta åstadkoms genom ökade krav på operatörerna att bevara trafikuppgifter.

Lokaliseringsuppgifter

Med lokaliseringsuppgift avses uppgifter som visar den geografiska positionen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst (prop. 2002/03:110 s. 260). En lokaliseringsuppgift kan vara en trafikuppgift och följer i så fall de regler som gäller för trafikuppgifter. Den behöver emellertid inte vara det (jfr 6 kap. 9 §). Till lokaliseringsuppgifter som samtidigt är trafikuppgifter hör framför allt information om i vilken cell i ett cellulärt uppbyggt mobilkommunikationssystem (som GSM) som en användare befinner sig vid ett visst tillfälle när utrustningen utnyttjas (a. prop. s. 260 f).

Sådana lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter får enligt huvudregeln i 6 kap. 9 § lagen om elektronisk kommunikation behandlas endast sedan de har avidentifierats. De får också under vissa förutsättningar behandlas, om användaren eller abonnenten har gett sitt samtycke till behandlingen.

Lokaliseringsuppgifter får lämnas till polisen eller till en regional alarmeringscentral i samband med nödsamtal (6 kap. 13 §). I övrigt har operatörer ingen skyldighet att lämna ut lokaliseringsuppgifter som inte är trafikuppgifter till brottsbekämpande myndigheter. Den generella tystnadsplikten gäller således för sådana uppgifter.

Man kan fråga sig om lokaliseringsuppgifter, som inte samtidigt är trafikuppgifter, får hämtas in genom husrannsakan och beslag eller genom editionsföreläggande, eftersom uppgifter av det slaget faller utanför det område som exklusivt regleras av rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Formellt torde det inte finnas något hinder mot detta. Teknikutvecklingen gör det möjligt att hämta in sådana uppgifter om de är lagrade, men lagstiftaren har aldrig tagit ställning till i vilken utsträckning det bör få ske. Konventionens regler tar dock endast sikte på lokaliseringsuppgifter som samtidigt är trafikuppgifter, varför frågan om tillgången till andra lokaliseringsuppgifter faller utanför uppdraget.

Uppgifter om abonnemang

Enligt artikel 18 punkt 1 b skall tjänsteleverantörer kunna åläggas att lämna ut abonnemangsuppgifter. Med abonnemangsuppgifter avses i detta sammanhang uppgifter som en tjänsteleverantör har och som hänför sig till andra uppgifter om dennes abonnenter än trafikuppgifter och uppgifter om innehållet i telemeddelanden. Genom uppgifterna skall det kunna fastställas bl.a.

- vilken typ av kommunikationstjänst som har använts och

- abonnentens identitet, postadress eller annan geografisk adress, telefonnummer och annat accessnummer samt
- var kommunikationsutrustningen finns.

Skyldigheten omfattar även den som abonnerar på eller på annat sätt utnyttjar gratistjänster.

Enligt 6 kap. 22 § första stycket 2 lagen om elektronisk kommunikation har en operatör, utan hinder av tystnadsplikten, skyldighet att lämna bl.a. polis och åklagare uppgift om abonnemang. Regleringen infördes för att tillgodose myndigheternas behov av att, på en avreglerad telemarknad, få uppgifter om hemliga telefonabonnemang (SOU 1992:70 s. 327 f och prop. 1992/93:200 s. 162 f). Med abonnemangsuppgifter åsyftas främst uppgifter om abonnentens namn, adress, yrke eller titel och telefonnummer. Även andra uppgifter, t.ex. abonnemangets form, kan ingå i begreppet. Uppgift om den s.k. PUK-koden, som knyter samman abonnemanget med en viss telefon, anses också utgöra en uppgift om abonnemang.

Som tidigare har framhållits uppfyller regeln kraven i artikel 18 punkt 1 b. Vad som är av intresse här är emellertid avgränsningen mellan vad som är abonnemangsuppgifter, å ena sidan, och uppgifter om ett särskilt telemeddelande, å den andra.

Är IP-nummer abonnemangsuppgifter?

Som tidigare har redovisats (avsnitt 6.5.3) har operatörer uppgiftsskyldighet gentemot brottsbekämpande myndigheter i två fall. Det ena avser abonnemangsuppgifter och det andra avser uppgifter som rör ett särskilt telemeddelande (ej innehållet i detta). Beteckningen trafikuppgift används inte i detta sammanhang.

Det har med tiden kommit att diskuteras vad som inryms i begreppet abonnemang. Enligt uppgift tolkas bestämmelsen olika av operatörerna. Det råder t.ex. olika uppfattningar om hur man skall betrakta ett IP-nummer.

Det finns två typer av IP-nummer. Den ena typen är fasta IP-nummer. Dessa kan jämföras med vanliga teleadresser och vållar

således inga problem. Det förhåller sig annorlunda med dynamiska IP-nummer, som är den tillfälliga adress som en dator tilldelas när den kommunicerar med andra datorer. I fortsättningen diskuteras endast dynamiska IP-nummer.

Frågan är om ett dynamiskt IP-nummer är en uppgift om abonnemanget eller en uppgift om ett särskilt telemeddelande. I båda fallen skall uppgiften lämnas ut, men det krav som ställs på brottets svårhetsgrad är olika. För att operatören skall vara skyldig att lämna uppgift om abonnemanget räcker det att det aktuella brottet kan antas leda till annan påföljd än böter. Uppgifter om ett särskilt telemeddelande förutsätter att minimistraffet för brottet är fängelse två år. Det har därför stor praktisk betydelse om en viss uppgift är att anse som en abonnemangsuppgift eller ej.

Det kan anföras argument för båda uppfattningarna. Vad som talar för att uppgift om IP-nummer skall anses vara en abonnemangsuppgift är att IP-numret är det ”alias” under vilket en enskild abonnent kommunicerar via Internet vid en viss tidpunkt, och att det därför kan jämföras med uppgift om abonnemang. Å andra sidan kan detta också anföras som ett argument för den motsatta ståndpunkten, nämligen att abonnemang avser ett mera permanent förhållande mellan kund och företag, medan IP-numret är en momentan uppgift för att identifiera ett visst kommunikationstillfälle. Uppgifter om enskilda kommunikationer är typiskt sett att hänföra till trafikuppgifter, och trafikuppgifter är i sin tur uppgifter om enskilda telemeddelanden.

Telelagsutredningen ansåg att uppgifter om när och mellan vilka abonnemang som ett telemeddelande har utväxlats var att hänföra till begreppet uppgift om ett telemeddelande (SOU 1992:70 s. 328). Departementschefen anslöt sig till denna uppfattning (prop. 1992/93:200 s. 163 och 310).

Förarbetena ger, utöver detta, inte någon ledning för var gränsen går mellan vad som är en uppgift om ett abonnemang och vad som är en uppgift om ett telemeddelande. Begreppet får därför tolkas med utgångspunkt i vanliga tolkningsdata. I den paragraf som reglerar operatörers skyldighet att lämna uppgifter till

de brottsbekämpande myndigheterna anges en rad andra myndigheter som också har rätt att få uppgifter om abonnemang samt de ändamål för vilka uppgifterna i fråga får lämnas ut. Det är uppenbart att det i dessa senare fall är uppgifter angående innehavarens identitet, adress och telefonnummer som är av intresse. Det ligger därför närmast till hands att anse att begreppet abonnemangsuppgift i punkt 2 inte omfattar andra uppgifter än sådana som rör det permanenta arrangemanget mellan abonnenten och operatören.

Med den utgångspunkten torde en uppgift om ett dynamiskt IP-nummer vara att anse som en uppgift om ett särskilt telemeddelande, inte om abonnemanget. För den tolkningen talar, som tidigare har nämnts, det förhållandet att abonnenten normalt tilldelas ett nytt IP-nummer för varje kommunikationstillfälle. Härtill kommer att med den definition av trafikuppgifter som används i konventionen det inte torde råda något tvivel om att ett IP-nummer är en trafikuppgift i konventionens mening.

De nuvarande reglerna i lagen om elektronisk kommunikation innebär med denna tolkning att det krävs att brottet har ett minimistraff på två års fängelse för att ett dynamiskt IP-nummer skall få lämnas ut. En så begränsad tillgång till uppgifter av detta slag uppfyller inte kraven i konventionen.

En ny regel om röjande av trafikuppgifter

Det bör av skäl som redovisats tidigare (avsnitt 11.3.3) införas en ny regel om röjande av trafikuppgifter i lagen om elektronisk kommunikation. Regeln bör placeras som en ny punkt i 6 kap. 22 §, som innehåller övriga regler om uppgiftsskyldighet.

Regeln bör utformas som en skyldighet för operatörer att lämna uppgifter rörande ett visst utpekat telemeddelande (dock inte innehållet i detta). De uppgifter som avses är trafikuppgifter, i förekommande fall innefattande lokaliseringsuppgifter. Uppgiftsskyldigheten skall inte vara generell utan skall avse ett visst utpekat telemeddelande. Bestämmelsen är således inte avsedd att ge underlag för allmänt informationssamlande.

Uppgiftslämnandet skall vidare vara nödvändigt för att ett visst meddelandes väg skall kunna spåras och för att de tjänsteleverantörer som har medverkat i överföringen skall kunna identifieras. Om dessa uppgifter redan är tillgängliga på annat sätt, t.ex. på grund av tillstånd till hemlig teleavlyssning eller hemlig teleövervakning, skall uppgifterna inte lämnas ut.

Samma lösning bör väljas som vid uppgiftslämnande enligt andra punkter i paragrafen, nämligen att det är den som begär att få ut uppgiften som bedömer om uppgifterna är nödvändiga (se prop. 1992/93:200 s. 163 f).

En viktig fråga är om uppgiftslämnandet skall avse alla typer av brott eller endast vissa brott. Övriga bestämmelser om uppgiftslämnande till brottsbekämpande myndigheter är generellt tillämpliga men innehåller krav på att brottet skall vara av viss svårhetsgrad. Ett motsvarande krav bör ställas även i dessa fall. Eftersom uppgifterna skall avse enstaka, särskilt utpekade kommunikationstillfällen är det inte nödvändigt att ha en fullt så snäv begränsning som i punkten 3. En lämplig avvägning kan vara att endast tillåta uppgiftslämnande för brott för vilka det kan följa fängelse i ett år. Det innebär samma straffskala som för bl.a. häktning. Med den valda lösningen tillgodoses kravet på att uppgifter skall kunna lämnas beträffande de brott som anges i artiklarna 2-11.

En annan fråga är om man bör ha samma krets av mottagare som i övriga bestämmelser om uppgiftslämnande. De som för närvarande får begära uppgifter med stöd av punkterna 2 och 3 anges i paragrafen som ”åklagarmyndighet, polismyndighet eller annan myndighet som skall ingripa mot brottet”. Den sistnämnda formuleringen innefattar bl.a. andra brottsbekämpande myndigheter som tullverket och skattebrottsenheterna. Det är oklart vilka myndigheter som därutöver har rätt att få del av uppgifterna (se SOU 1999:53 s. 139 f och prop. 2001/02:191 s. 52).

Eftersom trafikuppgifter får anses vara särskilt integritetskänsliga är det angeläget dels att regeln är så tydlig som möjligt, dels att kretsen av myndigheter som har rätt att få del av upp-

gifterna inte görs vidare än nödvändigt. De brott där det kan bli aktuellt att snabbt följa ett telemeddelandes väg är framför allt dataintrång, barnpornografibrott och vissa upphovsrättsliga brott samt sådana brott av rasistisk och främlingsfientlig natur som behandlas i tilläggsprotokollet. Brott av nu nämnda slag utreds av polis och åklagare. Uppgiftslämnandet bör därför begränsas till åklagarmyndigheter och polismyndigheter.[49] Om det senare skulle visa sig finnas ett praktiskt behov av det kan kretsen av myndigheter som har rätt till uppgifter utökas.

Som tidigare har nämnts framhålls i artikel 17 att åtgärderna skall förenas med tillräckliga rättssäkerhetsgarantier. Enligt JO:s uppfattning skall, av rättssäkerhetsskäl, frågan om uppgifter om telemeddelanden skall inhämtas som ett led i en förundersökning alltid underställas förundersökningsledaren, för att denne skall kunna ta ställning till om åtgärden är motiverad (JO 1998/99 s. 95). Om uppgiftsskyldigheten utvidgas på det nu föreslagna sättet blir det ännu viktigare att frågan om att hämta in uppgifter avgörs på en tillräckligt hög nivå. Den av JO förordade lösningen ter sig då lämplig.

11.8.4 Skyldighet att lämna upplysningar

Bedömning: Några nya regler som ålägger en person med särskild kunskap om ett visst datorsystem att lämna information som underlättar verkställandet av tvångsmedel bör inte införas.

Nuvarande regler

Enligt artikel 19 punkt 4 skall en person som har kunskap om ett datorsystems funktion eller dess säkerhetsåtgärder kunna föreläggas att, i den mån det är skäligt, lämna information som är

[49] Tullverket kan i och för sig utreda brott som avser in- eller utförsel av barnpornografi, men i de fall där det kan bli aktuellt med röjande av trafikuppgifter torde förundersökningen ledas av åklagare.

nödvändig för att möjliggöra användningen av husrannsakan och beslag. Syftet med bestämmelsen är få fram uppgifter från personer som är särskilt förtrogna med det datorsystem som är aktuellt, inte att ålägga en allmänt datakunnig person några extra förpliktelser att tillhandagå myndigheterna.

Varje medborgare, som kan antas ha upplysningar av betydelse för utredningen, är enligt 23 kap. 6 § RB skyldig att låta sig förhöras under en förundersökning. Han är däremot inte skyldig att yttra sig. Han är inte heller underkastad sanningsplikt, vilket är fallet vid vittnesförhör inför domstol.

Om den som förhörs tillfrågas om en uppgift som omfattas av en författningsreglerad tystnadsplikt som kan brytas vid ett vittnesförhör inför rätta anses han också ha rätt att lämna uppgiften vid förhör under förundersökning. Ytterst är det dock, som framgått ovan, förhörspersonen själv som avgör om, och i så fall i vilken utsträckning, han vill lämna uppgifter.

Bestämmelsen i 23 kap. 6 § RB innebär således inte att någon kan åläggas att lämna en viss uppgift.

Även under en förundersökning kan åklagaren emellertid kräva att det hålls vittnesförhör inför rätta. Vid ett sådant förhör, som regleras i 23 kap. 13 § RB, gäller samma skyldighet för ett vittne att uttala sig som vid ett vanligt vittnesförhör. Ett vittnesförhör under förundersökning förutsätter dels att den som skall höras har vägrat att yttra sig, dels att det är av synnerlig vikt för utredningen att han redan under förundersökningen hörs som vittne, dels att det finns någon som är skäligen misstänkt. Målsägande och misstänkt kan inte underkastas förhör enligt 23 kap. 13 § RB. Utrymmet för vittnesförhör under förundersökning är alltså begränsat och sådana förhör förekommer mycket sällan i praktiken.

Datastraffrättsutredningen föreslog att det skulle införas en möjlighet att förelägga den som kan antas ha särskild kännedom om ett visst datasystem att tillhandahålla upplysningar för att underlätta verkställigheten av beslut om husrannsakan (SOU 1992:110 s. 416). Förslaget har inte lett till lagstiftning.

Bedömning

Regleringen av tystnadsplikt ställd i relation till skyldigheten att medverka i en förundersökning utgör grundpelare i den svenska processlagstiftningen. Konventionen lämnar ett visst utrymme för att, när den nationella lagstiftningen inte gör det möjligt att i alla avseenden exakt överföra konventionsreglerna, välja andra lösningar, så länge de tillfredsställer de uppställda kraven.

I de fall där ett intrång har ägt rum utan medverkan av ägaren/brukaren av ett datorsystem torde denne i eget intresse bidra med alla de upplysningar som kan behövas för att underlätta verkställigheten av tvångsåtgärder. Det kan därför förutsättas att en målsägande som drabbas av husrannsakan antingen själv eller genom ombud frivilligt lämnar de upplysningar som kan krävas för att minimera intrånget och risken för skador på utrustning och information. Målsäganden (eller ett ombud för denne) kan också tillåtas att närvara vid husrannsakan (28 kap. 7 § tredje stycket RB). Något behov av ytterligare regler som tar sikte på målsägande, torde därför inte behövas.

Ett föreläggande mot någon som är misstänkt kan, av skäl som har utvecklats i avsnitt 11.5.1, inte godtas.

Den tredje kategori som kan beröras av frågan är vittnen. Möjligheten att vid vittnesförhör inför rätta utverka uppgifter får anses utgöra en tillräcklig garanti för att, i den mån det är skäligt, få fram de uppgifter som krävs av en helt utomstående.

Några särskilda lagstiftningsåtgärder bör därför inte vidtas.

11.9 Internationell rättslig hjälp

11.9.1 Rättslig hjälp med nya tvångsåtgärder m.m.

Förslag: Frysning av elektronisk kommunikation, kvarhållande av försändelse och kvarhållande av elektronisk post räknas upp bland de straffprocessuella tvångsmedel som får användas vid internationell rättslig hjälp. Det bör ställas krav på dubbel straffbarhet för de nu angivna hemliga tvångsmed-

len. Förbud mot att rubba elektronisk bevisning anges också bland de tvångsmedel med vilka Sverige ger rättslig hjälp. I princip krävs dubbel straffbarhet, men i förhållande till medlemsländerna i den Europeiska unionen och vissa andra länder bör det kravet mjukas upp, i likhet med vad som är fallet vid husrannsakan och beslag. Röjande av trafikuppgifter räknas också upp bland de åtgärder som Sverige ger hjälp med.

Allmänt om behovet av lagstiftningsåtgärder

Som framgått tidigare är lagstiftningen om internationell rättslig hjälp allmänt sett väl anpassad för att möta kraven i konventionen när det gäller befintliga tvångsmedel och andra utredningsåtgärder. I det föregående har emellertid olika förslag till förändringar framför allt på det processrättsliga området presenterats. En förutsättning för att de nya åtgärderna skall kunna användas på begäran av andra stater är att de täcks av regler i lagen om internationell rättslig hjälp. Det krävs därför följdändringar i denna.

Utvidgning av tillämpningsområdet

Reglerna om internationell rättslig hjälp omfattar redan i dag hjälp bl.a. med hemlig teleavlyssning och hemlig teleövervakning. Sedan tillämpningsområdet för dessa tvångsmedel utvidgats gäller utvidgningen automatiskt även i fråga om rättslig hjälp.[50] De ändringar i lagen om internationell rättslig hjälp som har föreslagits som ett led i anpassningen till 2000 års EU-konvention (se avsnitt 6.13.1) innebär också en utvidgning. Dessa ändringar underlättar dock bara möjligheterna att lämna och få rättslig hjälp med de redan befintliga hemliga tvångsmedlen på teleområdet.

Om frysning av elektronisk kommunikation införs som ett nytt tvångsmedel krävs det ändring i lagen om internationell

[50] Övergångsbestämmelserna innebär dock en viss begränsning, se avsnitt 11.12.3.

rättslig hjälp för att detta tvångsmedel skall kunna användas på begäran av en annan stat. Uppräkningen i 1 kap. 2 § lagen om internationell rättslig hjälp av tvångsåtgärder som får användas som ett led i verkställandet av en begäran om rättslig hjälp är nämligen uttömmande (prop. 1999/2000:61 s. 188). För att uppfylla Sveriges åtaganden enligt konventionen är det således nödvändigt att införa bestämmelser i lagen om internationell rättslig hjälp om frysning av elektronisk kommunikation. Av samma skäl bör förbud mot att rubba bevisning i elektronisk form räknas upp bland tvångsåtgärderna i 1 kap. 2 §. Röjande av trafikuppgifter (se avsnitt 11.8.3) är inte någon tvångsåtgärd och det kan därför inte sägas vara något absolut krav att åtgärden anges i paragrafen. Sverige kan nämligen enligt denna lämna även annan hjälp som inte kräver tvång. Vissa av de åtgärder som räknas upp i paragrafen är emellertid inte några tvångsmedel. Som exempel kan nämnas förhör. Eftersom det finns starka sakliga skäl att i uppräkningen ange sådana åtgärder som kan behöva specialregleras, bör även röjande av trafikuppgifter tillhöra de åtgärder som omnämns särskilt. Husrannsakan i IT-miljö faller in under begreppet husrannsakan och förslaget i denna del kräver därför inga ändringar i lagen om internationell rättslig hjälp.

När lagen om internationell rättslig hjälp år 2000 ersatte flera äldre lagar, bland dem lagen (1975:295) om användning av vissa tvångsmedel på begäran av främmande stat (tvångsmedelslagen), var avsikten att alla de tvångsmedel som tidigare hade kunnat användas på begäran av en annan stat skulle kunna utnyttjas även i fortsättningen (a. prop. s. 79). Ett sådant tvångsmedel var kvarhållande av försändelse enligt 27 kap. 9 § RB, vilket framgick genom en uttrycklig hänvisning i 7 § tvångsmedelslagen till den bestämmelsen. Det framgår av den allmänna motiveringen till lagen om internationell rättslig hjälp att avsikten var att kvarhållande av försändelse skulle ingå bland de tvångsmedel som får användas på begäran av en annan stat (a. prop. s. 123). Vid uppräkningen i lagtexten har detta tvångsmedel emellertid inte nämnts. Som tidigare har framhållits är uppräkningen av åtgärder som får vidtas med tvång uttömmande. Mot den bakgrunden

torde det vara svårt att hävda att kvarhållande av försändelse, som utgör ett självständigt tvångsmedel i förhållande till beslag, får användas som ett led i rättslig hjälp. För att möjliggöra rättslig hjälp med kvarhållande av elektronisk post och med post av traditionellt slag är det således nödvändigt att uttryckligen nämna båda dessa tvångsmedel i uppräkningen av åtgärder med vilka Sverige lämnar rättslig hjälp.

Dubbel straffbarhet

I lagen om internationell rättslig hjälp är utgångspunkten att användning av straffprocessuella tvångsmedel samt rättsmedicinsk obduktion kräver dubbel straffbarhet, men inte andra åtgärder som räknas upp i 1 kap. 2 § (se 2 kap. 2 §). När lagen infördes avskaffades tidigare gällande krav på dubbel straffbarhet för bl.a. förhör under förundersökning. I motiven framhölls att det internationella samarbetet underlättas om man kan begränsa kraven på dubbel straffbarhet (prop. 1999/2000:61 s. 105). I fråga om straffprocessuella tvångsmedel ansågs det dock att Sverige i princip bör behålla kravet på dubbel straffbarhet, eftersom det är tveksamt om man bör utsätta enskilda för så ingripande åtgärder om det inte är fråga om en gärning som är straffbar i Sverige (a. prop. s. 106). Kravet på dubbel straffbarhet måste ses mot bakgrund bl.a. av att lagstiftningen medger rättslig hjälp även med de mest integritetskänsliga tvångsmedel som förekommer i svensk rätt.

Undantag från kravet på dubbel straffbarhet har gjorts för husrannsakan och beslag på begäran av en annan stat i den Europeiska unionen eller inom Norden. I förhållande till dessa stater är det tillräckligt att det för gärningen kan dömas till fängelse i den ansökande staten (4 kap. 20 §).

Frågan är om de nya tvångsåtgärder som föreslås bör vara underkastade det generella kravet på dubbel straffbarhet eller om någon annan lösning bör väljas. Under de allra senaste åren har nämligen synen på dubbel straffbarhet kommit att ändras. Redan tidigare har man, på grund av de stora likheterna mellan de nor-

diska rättssystemen, i det straffrättsliga samarbetet inom Norden godtagit tvångsmedelsbeslut fattade i andra länder utan att ställa krav på dubbel straffbarhet. Utvecklingen av det straffrättsliga samarbetet inom den Europeiska unionen går nu i samma riktning. Numera verkställs i allt större utsträckning beslut fattade av myndigheter i en annan medlemsstat på grundval av ömsesidigt erkännande av beslut om straffprocessuella åtgärder. Sammanfattningsvis kan således konstateras att kravet på dubbel straffbarhet inte upprätthålls lika konsekvent som tidigare.

Konventionen, som kan komma att få en bred anslutning såväl inom som utanför den Europeiska unionen, lägger inte något hinder i vägen mot krav på dubbel straffbarhet (artikel 25 punkt 5). Däremot innebär konventionen att kravet på dubbel straffbarhet skall anses uppfyllt oberoende av hur brottet rubriceras i den anmodade staten, så länge gärningen är kriminaliserad. Att gärningen straffmässigt värderas olika får således inte hindra att kravet på dubbel straffbarhet anses uppfyllt. En annan sak är att det begärda tvångsmedlet kanske ändå inte kan användas, beroende på de krav på brottets svårhetsgrad, misstanke m.m. som ställs i den svenska lagstiftningen.

Frysning av elektronisk kommunikation utgör ett kort interimistiskt förstadium till mycket integritetskänsliga tvångsmedel, beträffande vilka det inte ens har diskuterats att man skulle kunna ge avkall på kravet på dubbel straffbarhet. Detta talar med styrka för att dubbel straffbarhet bör krävas för frysning.

Kvarhållande av försändelse räknas också till de hemliga tvångsmedlen. Samma skäl som motiverar att man beträffande andra hemliga tvångsmedel ställer upp krav på dubbel straffbarhet gör sig gällande vid kvarhållande av försändelse och kvarhållande av elektronisk post.

Åtgärden att förbjuda rubbande av bevisning i elektronisk form är mindre ingripande för den enskilde än exempelvis ett beslag. Åtgärden är emellertid avsedd att kunna utgöra ett förstadium till beslag. Därmed bör samma regler gälla som för beslag, dvs. ett generellt krav på dubbel straffbarhet. I förhållande till vissa länder är dock detta krav mildrat genom bestämmel-

serna i 4 kap. 20 § lagen om internationell rättslig hjälp. Ett motsvarande undantag bör göras för förbud mot rubbande av bevisning i elektronisk form.

Att med stöd av en operatörs skyldighet enligt lagen om elektronisk kommunikation inhämta uppgifter om telemeddelanden är inte något straffprocessuellt tvångsmedel. Frågan är om det bör krävas dubbel straffbarhet för en sådan åtgärd. Vad som talar för att man bör ställa upp krav på dubbel straffbarhet är främst att de uppgifter som röjs är av integritetskänslig art och att åtgärden har stora likheter med hemlig teleövervakning för förfluten tid. För hemlig teleövervakning krävs, som nyss har nämnts, dubbel straffbarhet. Vad som kan tala mot krav på dubbel straffbarhet är framför allt den nyss redovisade allmänna inställningen i svensk rätt att man så långt möjligt bör undvika sådana krav. Den inställningen genomsyrar också konventionen. Vidare måste det i så fall övervägas om den redan existerande möjligheten att, med stöd av 1 kap. 2 § andra stycket lagen om internationell rättslig hjälp i brottmål, bistå ett annat lands myndigheter med sådana uppgifter också bör omfattas av krav på dubbel straffbarhet.

Det är bäst förenligt med konventionens anda att inte ställa upp krav på dubbel straffbarhet annat än när det är nödvändigt med hänsyn till redan existerande principer i den nationella rätten. Eftersom det redan i dag är möjligt att – efter sekretessprövning – utan krav på dubbel straffbarhet till en annan stat överlämna uppgifter som har röjts med stöd av reglerna i lagen om elektronisk kommunikation bör det inte ställas upp något krav på dubbel straffbarhet när uppgiftsskyldigheten för operatörer utökas.

11.9.2 Förfarandet vid rättslig hjälp

Förslag: Regler om vad en ansökan om frysning av elektronisk kommunikation skall innehålla och hur den skall handläggas tas in i 4 kap. lagen om internationell rättslig hjälp. Eftersom ärenden om frysning av elektronisk kommunikation

är brådskande skall, så snart en ansökan om rättslig hjälp med frysning kommer in, åklagare pröva om det finns förutsättningar för åtgärden. Ett beslut om frysning skall omgående underställas domstol. Mot bakgrund av den korta frist som föreslås gälla för handläggningen av frysningsärenden bör det inte krävas någon särskild framställning om rättslig hjälp med teleavlyssning eller hemlig teleövervakning i de fall frysning har begärts. Det krävs också ett undantag från kravet i rättegångsbalken på förstöring av information från hemlig teleavlyssning. Det bör vidare införas regler om förfarandet vid röjande av trafikuppgifter.

Allmänt om förfarandet

I konventionens artikel 27 preciseras vad en framställning om rättslig hjälp skall innehålla i de fall där det inte finns något tillämpligt internationellt avtal. Av sådan framställning skall framgå

- vilken myndighet som begär åtgärden,
- vilket brott som förundersökningen eller rättegången avser, med en kort summering av relevanta fakta,
- vilken lagrad datainformation som åtgärden skall avse och dess anknytning till brottet samt
- all tillgänglig information som kan identifiera den som ansvarar för den lagrade datainformationen eller ange var datorsystemet finns. Vidare skall behovet av åtgärden belysas och slutligen skall det framgå att staten avser att begära rättslig hjälp med husrannsakan, beslag eller liknande säkringsåtgärd eller med röjande av informationen.

I 2 kap. 4 § lagen om internationell rättslig hjälp finns det generella regler om vad en ansökan om rättslig hjälp skall innehålla som i stora delar motsvarar bestämmelserna i artikel 27. De generella reglerna i nämnda paragraf kompletteras sedan med bestämmelser i lagens fjärde kapitel om vad som krävs för ansökan om vissa specifika åtgärder. Dessa regler behöver kompletteras med anledning av att användningsområdet för rättslig hjälp utvidgas.

Särskilt om artiklarna 29 och 30

När en svensk myndighet mottar en framställning om rättslig hjälp med säkrande av bevisning skall enligt artikel 29 den skyndsamt vidta alla åtgärder för att säkra de angivna uppgifterna i enlighet med svensk lagstiftning. Eftersom den svenska lagstiftningen kan skilja sig från vad som gäller i den begärande staten är det viktigt att den som tar ställning till framställningen snabbt gör klart för sig vilken åtgärd som enligt svensk rätt kan aktualiseras och agerar med utgångspunkt i det.

För frysning av elektronisk kommunikation är det av avgörande betydelse att den eller de teleadresser som beslutet bör omfatta snabbt kan identifieras. För att förfarandet med frysning skall kunna leda till adekvata åtgärder bör ansökan därför innehålla uppgift om vilken teleadress som åtgärden skall avse eller andra uppgifter som kan bidra till att identifiera den (t.ex. IP-nummer eller adressen för elektronisk post), om den uppgiften är känd. Regler om vad en ansökan skall innehålla bör därför tas in i 4 kap. i lagen om internationell rättslig hjälp.

Vidare bör det, med hänsyn till att framställningar om rättslig hjälp normalt är brådskande, föreskrivas att åklagare skall ta ställning till om det finns förutsättningar för frysning av elektronisk kommunikation så snart en framställning om detta kommer in.

Om åklagaren finner att det finns grund för frysning av elektronisk kommunikation och beslutar om detta skall han, enligt de föreslagna reglerna i 27 kap. 21 a § RB, snarast underställa domstolen frågan om hemlig teleavlyssning eller hemlig teleövervakning. I dessa fall bör det inte krävas någon särskild framställning om rättslig hjälp med hemlig teleavlyssning eller hemlig teleövervakning, eftersom en sådan begäran får anses ligga redan i ansökan om säkrande, när det av ansökan framgår att det är uppgifter om ett telemeddelande eller om innehållet i ett telemeddelande som den rättsliga hjälpen rör.

Det kan emellertid hända att det som begärs säkrat kan säkras genom en annan åtgärd än frysning av elektronisk kommunikation, nämligen förbud mot rubbande av bevisning i elektronisk

form eller röjande av trafikuppgifter. Innehållet i framställningen får avgöra vilken åtgärd som skall väljas i det enskilda fallet.

Enligt artikel 29 i konventionen skall sådan datainformation som har säkrats på begäran av en annan stat bevaras under en tid som inte understiger sextio dagar. Syftet med detta är att den stat som har begärt åtgärden skall hinna överlämna en framställning om att få ut informationen. Förfarandet är alltså tänkt att ske i två steg.

I 27 kap 24 § RB regleras hur information som har hämtats in med stöd av reglerna om hemlig teleavlyssning skall hanteras. Upptagningar och uppteckningar skall granskas så snart som möjligt. De får bevaras bara i de delar de är av betydelse från brottsutredningssynpunkt.[51] Syftet med bestämmelsen är att material som är särskilt integritetskänsligt snabbt skall kunna förstöras om det inte verkligen behövs. Det finns inget undantag från kraven på snabb granskning och förstörande.

Det ligger i sakens natur att den som på begäran av en annan stat genomför telefonavlyssning inte kan bedöma vad som är av intresse för den andra statens utredning. Det krävs därför en särskild regel som gör undantag från kraven på granskning och förstörande i fråga om material från hemlig teleavlyssning som hämtas in på en annan stats begäran. En sådan bestämmelse kan lämpligen placeras i 4 kap. 25 § lagen om internationell rättslig hjälp.[52]

Det följer av 2 kap. 9 § lagen om internationell rättslig hjälp att det kan ställas upp villkor exempelvis om att material från hemlig teleavlyssning skall förstöras efter användandet (se prop. 1999/2000:61 s. 147).

Artikel 29 förutsätter, som nyss har nämnts, ett förfarande i två steg, där informationen först begärs säkrad och senare begärs utlämnad. Det finns dock inget som hindrar att framställningen

[51] I Ds 2003:13 har föreslagits att regeln skall ändras, som ett led i regleringen av användning av överskottsinformation. Det förslaget har inte beaktats i denna promemoria.

[52] Ett motsvarande förslag till ändring har lagts fram i Ds 2004:50 (s. 226 ff). Den regeln har getts en mera generell utformning för att kunna tillgodose krav i olika konventioner och andra överenskommelser. Det förslaget innebär att material från hemlig teleavlyssning kan komma att bevaras under längre tid än vad krävs enligt åtagandena i konventionen om IT-relaterad brottslighet och som följer av förslagen i denna promemoria.

om säkrande också innehåller en anhållan om att resultatet av säkringsåtgärden skall överlämnas till den begärande staten.

Den föreslagna regeln i 4 kap. 25 § innebär endast ett undantag från skyldigheten att snabbt granska och förstöra material från hemlig teleavlyssning. Därför krävs det också en regel om den fortsatta hanteringen av material som har säkrats med stöd av artikel 29. Regeln kan lämpligen utformas på det sättet att materialet får bevaras under sextio dagar, i avvaktan på en framställning från den andra staten om att få del av uppgifterna. Om någon ansökan om rättslig hjälp med att få del av uppgifterna inte har kommit in under den tiden skall uppgifterna förstöras. Detsamma skall gälla om uppgifterna inte lämnas ut, t.ex. därför att säkrandet har omfattat fler uppgifter än vad framställningen om att få del av uppgifterna sedermera avser. Har ansökan kommit in i tid får uppgifterna bevaras till dess att ställning har tagits till begäran. De bör få bevaras längst till dess att ärendet om rättslig hjälp redovisas till den andra staten enligt 2 kap. 17 § lagen om internationell rättslig hjälp.

En av de frågor som regleras särskilt i konventionen är skyndsamt röjande av trafikuppgifter (artikel 30). Den anmodade staten skall, om den i samband med säkrandet av trafikuppgifter angående ett visst utpekat telemeddelande upptäcker att en tjänsteleverantör i en annan stat har medverkat i överföringen av meddelandet, skyndsamt meddela detta och samtidigt röja en tillräcklig mängd trafikuppgifter för att meddelandet skall kunna spåras. Även om inhämtande av trafikuppgifter med stöd av lagen om elektronisk kommunikation inte är ett tvångsmedel bör förfarandet ändå regleras i 4 kap. lagen om internationell rättslig hjälp. Visserligen har man undvikit att i lagen ta in regler som inte är allmängiltiga utan hänför sig till en viss överenskommelse, men i detta fall är regleringen central för den rättsliga hjälp som ges. Vidare är det fråga om uppgifter för vilka sekretess gäller. Det är då en fördel med en lagregel som tydligt anger när uppgifter av detta slag får lämnas till en annan stat.

Förhållandet mellan de nu föreslagna reglerna och förslagen i promemorian angående tillträde till 2000 års EU-konvention,

vilka har redovisats i avsnitt 6.13.1, är inte okomplicerat. Vad som är av särskilt intresse är förslagen i nyssnämnda promemoria om utvidgning av det rättsliga samarbetet i fråga om hemlig teleavlyssning och hemlig teleövervakning. Frågan är om dessa ändringar, om de genomförs, förändrar behovet av nya regler om frysning av elektronisk kommunikation. Vid en bedömning av den frågan måste först konstateras att de ändringar som har föreslagits med anledning av tillträdet till 2000 års EU-konvention inte påverkar möjligheterna att använda straffprocessuella tvångsmedel i ett svenskt förfarande, vilket är ett av huvudändamålen med konventionen om IT-relaterad brottslighet. Sistnämnda konvention syftar nämligen till att förbättra både den inhemska brottsbekämpningen och det internationella samarbetet. Vidare tillgodoser förslagen inte behovet av att som ett led i rättslig hjälp kunna få tillgång om trafikuppgifter utan samband med hemlig teleavlyssning eller hemlig teleövervakning. Förslagen i promemorian angående tillträde till 2000 års EU-konvention kan således inte ersätta de förslag som läggs fram här. De står inte heller i motsatsförhållande till de här framlagda förslagen.

Däremot skulle ett tillträde till 2000 års EU-konvention utan tvekan underlätta anpassningen till konventionen om IT-relaterad brottslighet i flera avseenden, beroende på att den förstnämnda konventionen generellt skapar bättre förutsättningar för rättsligt samarbete i fråga om hemliga tvångsmedel på teleområdet.

Skyndsamhetskravet

Konventionen ger möjlighet att skjuta upp verkställandet av en begärd åtgärd, om detta skulle inkräkta på brottmålsutredningar eller lagföring i den anmodade staten (artikel 27 punkt 5).

Lagen om internationell rättslig hjälp innehåller en regel om skyndsam handläggning (2 kap. 10 §), men inte någon regel som ger möjlighet att skjuta upp verkställandet av en framställning

om rättslig hjälp. Frågan är om det bör införas en uttrycklig regel om detta.

Vad som talar för en sådan bestämmelse är främst att lagtextens ovillkorliga skyndsamhetskrav inte ger utrymme för några undantag, hur sakligt välmotiverade de än må vara. I de fall där det har uppstått problem med verkställandet av rättslig hjälp har sannolikt frågan hittills lösts informellt efter kontakt med den ansökande staten. Ett undantag från det allmänna kravet på skyndsamhet kan göras beroende av att det har sin grund i en internationell överenskommelse. Numera innehåller konventioner och andra överenskommelser ofta bestämmelser som ger utrymme för att ta hänsyn till risken för negativa följder för brottsutredning och lagföring i den anmodade staten. I vissa äldre konventioner saknas emellertid sådana.

Vad som talar mot att skyndsamhetskravet förses med undantag är framför allt det förhållandet att enbart vissa konventioner innehåller undantag av det nu angivna slaget, samtidigt som en lagregel skulle få generell tillämplighet. Vidare bör noteras att lagstiftaren vid tillkomsten av lagen om internationell rättslig hjälp fann att lis pendens inte längre bör hindra rättslig hjälp och att tidigare regler av den innebörden därför inte fördes över till den nya lagen.

Det finns således argument som talar såväl för som emot en uttrycklig regel. Eftersom det inte förefaller ha uppstått några tillämpningsproblem med det ovillkorliga skyndsamhetskravet talar övervägande skäl för att man bör behålla den nuvarande lösningen.

11.9.3 Övriga frågor

Förslag: Rikskriminalpolisens IT-brottsrotel bör utpekas som kontaktpunkt enligt artikel 35. Justitiedepartementet utpekas som centralmyndighet enligt artikel 27 punkt 2. Eftersom Sverige kommer att bistå andra länder med att snabbt säkra lagrad datainformation bör svenska myndigheter på

motsvarande sätt kunna begära att uppgifter som behövs för svensk förundersökning eller process säkras i ett annat land.

Nationell kontaktpunkt respektive centralmyndighet

Varje land skall, för att möjliggöra bl.a. att lagrade data snabbt kan säkras, peka ut en nationell kontaktpunkt som kan nås dygnet runt alla dagar i veckan. Som redovisats i avsnitt 6.13.1 finns det en enhet hos polisen (Rikskriminalpolisens IT-brottsrotel) som uppfyller kraven såväl på tillgänglighet som på IT-kompetens. Genom åklagarväsendets system för jour och beredskap kan enheten alltid nå en beslutsfattare i frågor som rör internationell rättslig hjälp. Enheten bör pekas ut som svensk kontaktpunkt enligt artikel 35.

Enligt artikel 27 punkt 2 skall varje land peka ut en centralmyndighet som mottar och sänder framställningar om rättslig hjälp i de fall där det inte finns någon bindande överenskommelse om rättslig hjälp mellan parterna. Justitiedepartementet fungerar redan som centralmyndighet i frågor om internationell rättslig hjälp och utlämning. Justitiedepartementet bör därför pekas ut som centralmyndighet enligt den nu angivna artikeln.

Svenska myndigheters möjlighet till rättslig hjälp

Regleringen i lagen om internationell rättslig hjälp bygger på den grundläggande principen att svenska myndigheter skall kunna begära rättslig hjälp med samma åtgärder som vi bistår andra länder med. De nya möjligheterna till samarbete i form av snabbt säkrande av datalagrade uppgifter bör därför avspeglas i lagen.

I 3 kap. 1 § lagen om internationell rättslig hjälp anges i vilken utsträckning de formella krav som Sverige ställer på en utländsk framställning om rättslig hjälp gäller när svenska åklagare begär motsvarande hjälp i ett annat land. Bestämmelsen bör kompletteras med hänvisningar till de nya reglerna i 4 kap.

Rättslig hjälp på yttrande- och tryckfrihetsområdena

Lagen om internationell rättslig hjälp är inte tillämplig på TF:s och YGL:s områden (se prop. 1999/2000:61 s. 73). Det innebär, som framgått av avsnitt 7.6.1, att Sverige för närvarande inte kan ge rättslig hjälp beträffande sådana brott som faller inom det grundlagsskyddade området. Frågan om möjligheterna att ge internationell rättslig hjälp inom det tryck- och yttrandefrihetsrättsliga området har, som redovisats där, utretts av Tryck- och yttrandefrihetsberedningen. Beredningen har föreslagit att det skall vara möjligt att lämna viss rättslig hjälp beträffande brott mot tryck- och yttrandefrihet (se närmare om detta i avsnitt 7.6.1). Någon lagstiftningsåtgärd är därför inte nödvändig i detta sammanhang.

11.10 Följdändringar i annan lagstiftning

11.10.1 Lagen om elektronisk kommunikation

Förslag: I lagen om elektronisk kommunikation görs de följdändringar som krävs med anledning av att ett nytt tvångsmedel, frysning av elektronisk kommunikation, införs. Vidare görs det ändringar för att skapa överensstämmelse med den nya regeln om kvarhållande av elektronisk post. En ny regel om röjande av trafikuppgifter införs. Dessutom flyttas definitionen av vad som är ett telemeddelande från lagen om elektronisk kommunikation till rättegångsbalken.

Lagen om elektronisk kommunikation innehåller vissa bestämmelser om hemlig teleavlyssning och hemlig teleövervakning som riktar sig till operatörer. Ett beslut om frysning av elektronisk kommunikation utgör ett förstadium till domstols beslut i fråga om hemlig teleavlyssning eller hemlig teleövervakning. Det är därför nödvändigt att i lagen om elektronisk kommunikation föra in regler om verkställighet av åklagares beslut om frysning av elektronisk kommunikation.

För att möjliggöra frysning krävs det en regel om undantag från huvudregeln att trafikuppgifter omedelbart skall utplånas eller avidentifieras. Redan i dag finns det vissa undantag. För det första får operatören under viss tid bevara de uppgifter som behövs för fakturering och betalning. För det andra får operatören bevara vissa uppgifter för marknadsföring, om abonnenten har samtyckt till det. Vad som främst är av intresse här är dock att regeln om utplånande och avidentifiering inte gäller

1. när en myndighet eller domstol behöver tillgång till sådana uppgifter för att lösa tvister,
2. för elektroniska meddelanden som omfattas av beslut om hemlig teleavlyssning eller hemlig teleövervakning eller
3. i den utsträckning uppgifterna behövs för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

För att en regel om frysning skall få avsedd effekt krävs det att frysning i detta avseende jämställs med beslut om hemlig teleavlyssning eller hemlig teleövervakning. Detta görs lämpligen genom ett tillägg i 6 kap. 8 §. Ett motsvarande undantag krävs för åtgärd enligt 27 kap. 9 a § RB (kvarhållande av elektronisk post).

Vidare måste operatörernas verksamhet bedrivas så att beslut om frysning av elektronisk kommunikation kan verkställas och så att verkställigheten inte röjs. Reglerna i 6 kap. 19 § måste därför kompletteras så att även beslut om frysning omfattas. En motsvarande komplettering krävs beträffande åtgärder enligt 27 kap. 9 a § RB.

Som har redovisats i avsnitt 11.8.2 krävs det motsvarande ändringar i 6 kap. 21 § för att operatörernas tystnadsplikt skall omfatta även frysning och kvarhållande av elektronisk post. Vidare måste röjande av trafikuppgifter regleras (avsnitt 11.8.3).

Med stöd av reglerna i lagen om elektronisk kommunikation kan en operatör på begäran bl.a. lämna ut trafikdata och lokaliseringsuppgifter till polis och åklagare. För att undvika en dubbelreglering bör föreskrivas att uppgifter som har varit föremål för frysning inte får lämnas ut med stöd av 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation.

Som framgått ovan (avsnitt 11.3.1) bör definitionen av vad som är ett telemeddelande flyttas till rättegångsbalken, eftersom den inte längre hör hemma i lagen om elektronisk kommunikation. Detta kräver en följdändring i 6 kap. 1 §, eftersom begreppet telemeddelande alltjämt används i några paragrafer i kapitlet.

Det bör i sammanhanget anmärkas att Beredningen för rättsväsendets utveckling också har lagt fram förslag till ändringar i 6 kap. 19 och 22 §§ lagen om elektronisk kommunikation (se SOU 2003:74). Ändringarna, som enbart rör frågan om vem som skall betala kostnaderna för verkställigheten av hemlig teleavlyssning och hemlig teleövervakning, saknar betydelse för de förslag som redovisas här. Vidare har det i promemorian om tillträde till 2000 års EU-konvention (se avsnitt 6.13.1) föreslagits vissa ändringar i 6 kap. 8 och 21 §§ lagen om elektronisk kommunikation. Inte heller dessa förslag till ändringar påverkar de i denna promemoria framlagda förslagen.

11.10.2 1952 års lag

Förslag: Den föreslagna regeln om frysning av elektronisk kommunikation skall gälla även för brott som omfattas av 1952 års lag. Det finns inte längre något behov av interimistiska beslut om hemlig teleavlyssning och hemlig teleövervakning om reglerna om frysning görs tillämpliga på lagen. Åklagares rätt att interimistiskt besluta om hemliga tvångsmedel på teleområdet bör därför tas bort.

För utredning av bl.a. brott mot rikets säkerhet har det ansetts nödvändigt med en lagstiftning som medger att straffprocessuella tvångsmedel kan användas i något större utsträckning än annars. I 1952 års lag finns det regler som dels utvidgar tillämpningsområdet för vissa tvångsmedel, dels innebär att det ställs mindre stänga krav i fråga om frister och liknande. I de avseenden 1952 års lag inte innehåller några undantag från rättegångsbalkens reglering gäller balkens regler automatiskt. Det innebär

att samtliga de förslag till ändringar som har redovisats tidigare kommer att gälla även vid brott som anges i 1952 års lag.

I avsnitt 11.4 har föreslagits nya regler om frysning av elektronisk kommunikation. Dessa innebär att en åklagare kan besluta om frysning, vilket medför att en operatör blir skyldig att bevara uppgifter om elektronisk kommunikation, i avvaktan på att domstol tar ställning till användningen av hemlig teleavlyssning eller hemlig teleövervakning. Med en sådan ordning finns det inte längre något behov av interimistiska beslut om hemliga tvångsmedel på teleområdet, eftersom frysningsbeslut i allt väsentligt ger samma praktiska resultat. Om man låter de nuvarande reglerna i 1952 års lag om åklagares rätt att fatta interimistiska beslut om hemliga tvångsmedel kvarstå oförändrade får man två parallella system som är tillämpliga på samma beslutsfattare, något som bör undvikas. En dubbelreglering kan också skapa problem vid verkställigheten. Av rättssäkerhetsskäl bör därför bestämmelsen i 5 § andra stycket om åklagares rätt att interimistiskt besluta om hemlig teleavlyssning och hemlig teleövervakning utgå.

11.10.3 Andra lagar med regler om hemliga tvångsmedel

Förslag: Den föreslagna regeln om frysning av elektronisk kommunikation blir generellt tillämplig. Åklagares rätt att interimistiskt besluta om hemlig teleavlyssning och hemlig teleövervakning enligt lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. bör därför tas bort. Det finns inte längre något behov av interimistiska beslut om dessa tvångsmedel om frysning införs. Fristen för att underställa domstol frågan om användning av tvångsmedel bör anpassas till vad som gäller enligt rättegångsbalken. Vidare föreslås en ändring av reglerna om kvarhållande som hör samman med den nya bestämmelsen om kvarhållande av elektronisk post. I fråga om de regler om hemlig teleavlyssning och hemlig tele-

övervakning som finns i lagen (1991:572) om särskild utlänningskontroll föreslås inga ändringar.

Det finns regler om hemlig teleavlyssning och hemlig teleövervakning också i annan lagstiftning. I 28 § lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. finns det en bestämmelse som ger åklagare möjlighet att interimistiskt besluta om hemliga tvångsmedel bl.a. på teleområdet. Åklagare får interimistiskt besluta om sådana tvångsmedel om det skulle innebära en fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen att inhämta rättens tillstånd. Åklagare eller undersökningsledare får på motsvarande sätt besluta om kvarhållande av försändelse. Ett beslut om hemligt tvångsmedel skall genast anmälas hos rätten, som skall pröva ärendet snabbt.

Av samma skäl som åklagares interimistiska beslutanderätt enligt 1952 års lag bör upphävas, eftersom bestämmelsen inte längre behövs när reglerna om frysning av elektronisk kommunikation införs, bör reglerna om interimistisk beslutanderätt i fråga om hemlig teleavlyssning och hemlig teleövervakning i den nu aktuella lagen upphävas. Vidare bör bestämmelsen även i övrigt anpassas. Kravet i 28 § på att ett åklagarbeslut omedelbart skall anmälas innebär att det i nämnda paragraf ställs strängare krav än i 27 kap. 21 a § RB i fråga om frysning, vilket inte bör vara fallet. Detta kan lösas genom en hänvisning till den sistnämnda bestämmelsen.

Vidare krävs det en ändring i fråga om rätten att besluta om kvarhållande av försändelse, med anledning av det nya tvångsmedlet kvarhållande av elektronisk post. Om den bestämmelsen inte ändras kommer en förundersökningsledare hos polisen att kunna besluta om kvarhållande såväl av traditionella försändelser som av elektronisk post. Detta skulle leda till en kraftig utvidgning av polisens behörighet att besluta om särskilt integritetskänsliga tvångsmedel. Den lämpligaste lösningen torde vara att låta åklagare fatta interimistiska beslut om kvarhållande av elektronisk post.

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns också i lagen (1991:572) om särskild utlänningskontroll. Dessa tvångsmedel, som beslutas av domstol på framställning av Rikspolisstyrelsen, har emellertid ett helt annat syfte eftersom de inte är avsedda för brottsutredning utan för att tillgodose behovet av särskilda spaningsåtgärder för att förebygga terrorism. Något skäl att ändra dessa regler med anledning av att frysning av elektronisk kommunikation införs finns inte.

11.11 Behovet av förbehåll m.m.

Förslag: Sverige bör, i fråga om konventionen, avge förklaring till artikel 3, som behandlar olovlig avlyssning, att möjligheten att ställa upp särskilt rekvisit utnyttjas. Till artikel 4, som avser systemstörning, bör ett förbehåll göras om att det för straffbarhet krävs att handlandet medför allvarlig skada. Vidare bör Sverige avge förbehåll enligt artikel 9 punkt 4 av innebörd att ringa barnpornografibrott undantas. Eftersom försök till bedrägligt beteende inte är straffbart krävs det förbehåll också för detta. Slutligen bör avges förbehåll enligt artikel 14 punkt 3 a av innebörd att hemlig teleövervakning endast får förekomma vid misstanke om brott med lägst sex månaders fängelse i straffskalan eller vid annat brott som anges i 27 kap. 19 § RB eller 1952 års lag och endast riktas mot den som är skäligen misstänkt.

I fråga om tilläggsprotokollet bör Sverige göra förbehåll enligt artikel 3 punkt 3 och artikel 5 punkt 2 b för etablerade principer om yttrandefrihet samt enligt artikel 6 punkt 2 b för kriminalisering av förringande eller förnekande av folkmord och brott mot mänskligheten.

11.11.1 Möjligheterna att göra förbehåll och avge förklaring

Konventionen

Enligt artikel 42 i konventionen får förbehåll göras i fråga om
- artikel 4, som behandlar datastörning (förbehåll om krav på allvarlig skada),
- artikel 6, som behandlar missbruk av brottshjälpmedel (dels förbehåll om krav på att innehav för att vara straffbart skall omfatta fler än ett hjälpmedel, dels förbehåll att artikeln till viss del inte skall tillämpas)
- artikel 9, som behandlar barnpornografi (förbehåll att helt eller delvis inte tillämpa punkterna 1 d och e och 2 b och c),
- artikel 10, som behandlar intrång i upphovsrätt och närstående rättigheter (förbehåll att i begränsad utsträckning välja andra åtgärder än straffansvar),
- artikel 11, som behandlar försök och medhjälp (förbehåll att helt eller delvis inte införa straffansvar för försök),
- artikel 14, som behandlar de processuella reglernas tillämplighet (dels förbehåll i fråga om för vilka brott hemlig teleövervakning skall tillämpas, dels förbehåll för att inte tillämpa hemlig teleavlyssning och hemlig teleövervakning inom vissa nät),
- artikel 22, som behandlar jurisdiktion (förbehåll i fråga om jurisdiktion när brottet begås bl.a. ombord på fartyg eller luftfartyg),
- artikel 29, som behandlar skyndsamt säkrande (förbehåll i fråga om grunden för att avslå en framställning om rättslig hjälp) och
- artikel 41 (förbehåll angående förhållandena inom en federal stat).

Vidare får en stat enligt artikel 40 avge förklaring att den begagnar sig av möjligheten att kräva ytterligare rekvisit enligt artiklarna 2, 3, 6 punkt 1 b, 7, 9 punkt 3 och 27 punkt 9 e.

Tilläggsprotokollet

Enligt tilläggsprotokollet gäller de förbehåll och förklaringar som har avgetts till konventionen också i förhållande till tilläggsprotokollet, om parten inte förklarar annat.

I fråga om tilläggsprotokollet får parterna avge förklaring att de använder sig av möjligheten att kräva särskilda rekvisit eller att avstå från kriminalisering beträffande

- artikel 3, som behandlar spridande av rasistiskt och främlingsfientligt material (förbehåll om krav på att materialet förespråkar, främjar eller uppmuntrar hat eller våld eller förbehåll hänförligt till etablerade principer om yttrandefrihet)
- artikel 5, som behandlar kränkning som är rasistiskt och främlingsfientligt motiverad (förbehåll om krav på att gärningen leder till att personen eller gruppen utsätts för hat, missaktning eller löje) och
- artikel 6, som behandlar förnekande, förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten (antingen förbehåll om krav på att förnekandet eller förringandet uppmanar till hat, diskriminering eller våld eller förbehåll att helt eller delvis inte införa straffansvar).

11.11.2 Vilka möjligheter till förbehåll och undantag bör utnyttjas?

Konventionen

Vid framförhandlandet av internationella konventioner är det oundvikligt att det tillskapas regler som kan vara svåra att förena med den svenska rättstraditionen och där det vid anpassningen till svensk lagstiftning ibland kan visa sig nödvändigt att utnyttja undantag och förbehåll av olika slag. Så långt möjligt bör detta dock undvikas.

Förslagen i denna promemoria har i största möjliga utsträckning utformats så att det inte skall behövas förbehåll eller undantag, eller så att dessa i varje fall kan minimeras. Vid en jämfö-

relse med lagstiftningsarbetet i Danmark och Norge kan noteras att båda länderna i olika utsträckning har funnit behov av att utnyttja möjligheterna till förbehåll eller reservationer. Detsamma gäller flera andra länder som för närvarande arbetar med frågor om ratificering och anpassning av den nationella rätten.

I fråga om de straffrättsliga reglerna bör i några fall möjligheten att ställa upp särskilda rekvisit eller att inte tillämpa konventionen på någon viss punkt utnyttjas.

Enligt artikel 3 får det vid kriminalisering av olovlig avlyssning ställas krav på särskilt uppsåt. Som redovisats i avsnitt 11.1.3 bör denna möjlighet begagnas. Sverige bör således avge förklaring till artikel 3.

Möjligheten att enligt artikel 4 punkt 2 ställa krav på att handlandet medför allvarlig skada bör också utnyttjas (avsnitt 11.1.2). Med den lösningen blir det inte nödvändigt att göra förbehåll enligt artikel 11punkt 3 för att försök till åverkan inte är straffbart. Sverige bör därför avge förbehåll till artikel 4.

Den nuvarande bestämmelsen om ringa barnpornografibrott har en straffskala som innebär att vissa av de tvångsmedel som konventionen förutsätter skall vara möjliga att använda inte är tillämpliga. Det är framför allt innehav i liten skala för eget bruk som brukar bedömas som ringa brott. I valet mellan att radikalt förändra straffskalan och att delvis göra undantag i enlighet med artikel 9 punkt 4 bör den senare lösningen väljas, särskilt mot bakgrund av att en översyn av straffskalorna för vissa brott, bland dem barnpornografibrott, nyligen har gjorts inom ramen för ett annat lagstiftningsärende (se avsnitt 6.5.3). Sverige bör således avge förbehåll att artikel 9 punkt 1 e inte tillämpas på barnpornografibrott som är ringa.

Den nuvarande lagstiftningen uppfyller, med några få undantag, kravet i artikel 11 punkt 2 på att försöksbrott skall vara kriminaliserade. Undantagen är vissa ringa brottsformer nämligen försök till

- dataintrång som är att anse som ringa och
- bedrägligt beteende.

Att ringa brottsformer har undantagits från kriminalisering på försöksstadiet ligger i linje med hur man i allmänhet har sett på vilka gärningar som bör kriminaliseras redan innan de har fullbordats. Det finns inte skäl att nu ändra på detta synsätt. Sverige bör därför använda sig av möjligheten i artikel 11 punkt 3 att avge förbehåll i fråga om båda brottstyperna.

Enligt artikel 14, som behandlar frågan om hur brett tillämpningsområde de processrättsliga reglerna skall ha, finns det möjlighet att avge förbehåll i två hänseenden som berör användning av hemliga tvångsmedel på teleområdet. Den ena möjligheten till förbehåll rör den generella tillämpligheten av sådana tvångsmedel som medger åtkomst till uppgifter om trafikdata, dvs. hemlig teleövervakning (artikel 14 punkt 3 a). Den andra rör undantag för meddelanden som överförs inom vissa nät (artikel 14 punkt 3 b).

Eftersom de processrättsliga bestämmelserna skall kunna tillämpas inte bara på brott som anges i konventionen utan på varje annan typ av brott som kan begås med hjälp av ett datorsystem är det nödvändigt att göra förbehåll enligt artikel 14 punkt 3 a för att hemlig teleövervakning endast får förekomma vid brott för vilka det är föreskrivet lägst sex månader fängelse eller för annat brott som anges i 27 kap. 19 § RB eller 1952 års lag, och endast riktas mot den som är skäligen misstänkt. Motsvarande undantag kommer då att gälla vid rättslig hjälp (artikel 33 punkt 1).

Med den ändring av undantaget för användning av hemliga tvångsmedel i vissa nät som har föreslagits ovan (avsnitt 11.7) torde det inte krävas något förbehåll enligt artikel 14 punkt 3 b.

Tilläggsprotokollet

Sveriges speciella reglering av yttrande- och tryckfrihet medför att förbehåll för etablerade principer om yttrandefrihet måste göras enligt artikel 3 punkt 3 och artikel 5 punkt 2 b. Förbehåll torde vara nödvändiga för att garantera den svenska särregleringen även i framtiden. Förbehållen bör avse att straffansvar inte

utkrävs om detta skulle strida mot den svenska regleringen av tryck- och yttrandefriheten.

Möjligheten att avge förbehåll enligt artikel 6 punkt 2 b bör, som utvecklats närmare i avsnitt 7.3.4, också användas. Förbehållet bör avse kravet på kriminalisering av förringande och förnekande av folkmord och brott mot mänskligheten, eftersom svensk rätt i övrigt uppfyller konventionskraven i nämnda artikel. Även om det inte torde krävas något formellt undantag för brott som faller under det grundlagsskyddade området, eftersom Sverige kan använda sig av möjligheten enligt ingressen att göra undantag för etablerade principer på yttrandefrihetsområdet, bör det för tydlighetens skull framgå att undantaget omfattar såväl allmänna brott som tryck- och yttrandefrihetsbrott.

11.12 Konsekvenser, kostnader och genomförande

11.12.1 Konsekvenser

Bedömning: En ratificering av konventionen kommer att få positiva effekter för brottsbekämpningen. Den påverkar däremot inte den kommunala självstyrelsen, sysselsättning och offentlig service i olika delar av landet, små företag, jämställdheten mellan kvinnor och män eller möjligheten att nå de integrationspolitiska målen.

Konventionen och tilläggsprotokollet innebär ett betydande steg framåt för möjligheterna att upptäcka, utreda och lagföra IT-relaterade brott. Ett utvidgat samarbete med de brottsbekämpande myndigheterna i andra länder kommer att få stor betydelse för effektiviteten i brottsbekämpningen inom detta område. Man kan vidare anta att allmän kännedom om möjligheterna till samarbete över gränserna kommer att minska brottsbenägenheten. En ratificering kommer därför att få positiva effekter.

Däremot medför en ratificering inga konsekvenser för

- den kommunala självstyrelsen,

- sysselsättning och offentlig service i olika delar av landet,
- små företag,
- jämställdheten mellan kvinnor och män eller
- möjligheten att nå de integrationspolitiska målen.

11.12.2 Kostnader

Bedömning: En ratificering av konventionen om IT-relaterad brottslighet medför i sig inga ökade kostnader för staten. Eftersom konventionen förutsätter en viss utvidgning av det straffbelagda området kan detta leda till fler brottsanmälningar, men kostnaderna för detta bedöms kunna finansieras inom ramen för befintliga medel. De ändrade reglerna om tvångsmedel och internationell rättslig hjälp bedöms också kunna finansieras inom ramen för befintliga medel. För operatörerna bedöms ändringarna endast ha marginella effekter.

Om Sverige ratificerar konventionen om IT-relaterad brottslighet medför detta i sig inte några ökade kostnader för staten. De författningsändringar som krävs med anledning av en ratificering, och som kan ha betydelse när det gäller kostnader, är dels utvidgningen av det straffbara området, dels ändrade regler om tvångsmedel. Det straffbara området utvidgas bara i mycket begränsad omfattning. Ändringarna kommer knappast att leda till någon nämnvärd ökning av antalet brottsanmälningar och påverkar därför bara kostnaderna marginellt. Eventuella kostnadsökningar bör därför kunna finansieras inom ramen för befintliga medel.

Det föreslagna nya tvångsmedlet frysning av elektronisk kommunikation utgör enbart ett förstadium till ansökan respektive beslut om hemlig teleavlyssning och hemlig teleövervakning. Det kan inte orsaka något merarbete för domstolarna, men däremot ett obetydligt merarbete för åklagare, som skall fatta beslut om frysning. Ett sådant beslut förutsätter emellertid att det finns skäl att ansöka om hemlig teleavlyssning eller hemlig teleöver-

vakning, och merarbetet blir därför marginellt. Övriga förslag till ändringar i 27 och 28 kap. RB torde bidra till effektivare förundersökningar, vilket är ägnat att minska kostnaderna.

Ett ökat internationellt samarbete kan komma att ställa ökade krav på arbetsinsatser inom åklagarväsendet. Mot detta skall dock ställas ökad effektivitet genom vidgade möjligheter att använda tvångsmedel och den vinst som det innebär att svenska åklagare i större utsträckning än tidigare kan få hjälp från andra länder.

Eventuella kostnadsökningar för förslagen på det processuella området och i fråga om rättslig hjälp bedöms mot den nu angivna bakgrunden kunna finansieras inom ramen för befintliga medel.

Som framgått ovan är det Säkerhetspolisen som ansvarar för myndigheternas verkställighetsåtgärder vid hemlig teleavlyssning och hemlig teleövervakning. Den nuvarande lagstiftningen bygger på att operatörerna svarar för de kostnader som följer av behovet av att anpassa de tekniska systemen så att hemliga tvångsmedel kan användas och att resultatet av tvångsmedelsanvändningen kan presenteras för de brottsbekämpande myndigheterna i omedelbart användbar form. Däremot betalar Säkerhetspolisen för verkställighet i form av inkoppling m.m. En ökad användning av dessa tvångsmedel kan därför leda till ökade kostnader för Säkerhetspolisen. Beredningen för rättsväsendets utveckling har emellertid nyligen föreslagit att operatörerna skall vara skyldiga att utföra dessa uppgifter utan kostnader för staten (SOU 2003:74 s. 253 ff). Regeringen har ännu inte tagit ställning till förslaget. Om beredningens förslag leder till lagstiftning minskar Säkerhetspolisens kostnader för verkställigheten avsevärt eftersom ersättningen till operatörer för år 2003 beräknas överstiga elva miljoner kronor (a.a. s. 252). Det finns anledning att här understryka vikten av att kostnadsfrågan löses så snart som möjligt. Ett genomförande av Beredningens förslag skulle underlätta genomförandet av de förslag som presenteras i denna promemoria.

Oavsett hur man löser den nu aktuella frågan kan konstateras att reglerna om frysning av elektronisk kommunikation inte kommer att leda till fler ärenden, men däremot till fler kontakter mellan Säkerhetspolisen och operatörerna. Däremot innebär införandet av kontroll av elektronisk post en utökning av de hemliga tvångsmedlen. Merkostnaderna uppvägs för Säkerhetspolisens del av en ökad effektivitet om tvångsmedlet används i den egna verksamheten. I de fall där Säkerhetspolisen endast ombesörjer verkställigheten torde kostnaderna öka. Eventuella kostnadsökningar bör dock kunna finansieras inom ramen för befintliga medel.

För operatörernas del innebär förslagen följande. Tystnadsplikten utvidgas, vilket inte i sig torde leda till några ökade kostnader. Den nya skyldigheten att röja trafikuppgifter torde, med dagens ersättningssystem, inte heller innebära några merkostnader för operatörerna eftersom det endast är fråga om lagrade uppgifter.

Den utökade anpassningsskyldigheten kan dock få betydelse. När det gäller frysning torde kravet på anpassning endast ha marginell betydelse eftersom det i huvudsak – sett från operatörernas perspektiv – är fråga om en ändring i beslutsstrukturen i fråga om tvångsmedel för vilka anpassningsskyldighet gäller sedan tidigare. Det enda som kan behövas är att utforma rutiner för att avvakta med att lämna ut frysningsuppgifter till dess att det finns ett domstolsbeslut.

Däremot innebär kontroll av elektronisk post att ett nytt tvångsmedel införs. Även i detta fall måste emellertid anpassningsskyldigheten ses i ljuset av de förpliktelser som operatörerna redan har. Det ingår redan i dag i deras skyldigheter att anpassa tekniken så att uppgifter om telemeddelanden i form av elektronisk post och om innehållet i sådana meddelanden kan ställas till polisens förfogande när det finns ett domstolsbeslut om hemlig teleövervakning respektive hemlig teleavlyssning. Vad som kan krävas med anledning av att kontroll av elektronisk post införs som ett särskilt tvångsmedel är därför enbart att den redan befintliga tekniken anpassas något. Mot den bakgrunden bedöms

operatörernas utökade anpassningsskyldighet endast få marginella effekter.

11.12.3 Genomförandet

Förslag: Förslagen bör genomföras så snart som möjligt. Ändringarna i brottsbalken, som innebär viss nykriminalisering, bör endast omfatta brott som har begåtts efter ikraftträdandet. Däremot bör det inte ges några särskilda övergångsbestämmelser för lagförslagen i övrigt, vilket innebär att de processrättsliga reglerna och möjligheten att lämna rättslig hjälp omfattar även brott som har begåtts före ikraftträdandet av den nya lagstiftningen.

Det är angeläget att förslagen genomförs så snart som möjligt.

Ändringarna i brottsbalken, som innebär nykriminalisering, bör inte gälla för brott som har begåtts före ikraftträdandet. En särskild övergångsbestämmelse av den innebörden bör införas.

Det normala är att processrättsliga regler ges omedelbar verkan. Av det skälet bör det inte införas några övergångsbestämmelser för ändringarna i rättegångsbalken och övriga lagändringar. Det innebär att möjligheten att använda tvångsmedel och att lämna rättslig hjälp omfattar även brott som har begåtts före ikraftträdandet. Det bör dock anmärkas att övergångsbestämmelserna i prop. 2002/03:74 om utvidgningar av tillämpningsområdet för hemliga tvångsmedel på teleområdet i sig innebär en begränsning. Dessa föreskriver nämligen att tillstånd till hemlig teleavlyssning och hemlig teleövervakning för förfluten tid inte får avse tid före ikraftträdandet.

12 Författningskommentar

12.1 Förslaget till ändringar i rättegångsbalken

9 kap

6 §
Paragrafen reglerar sanktionen för den som överträder ett yppandeförbud. I uppräkningen över vilka som kan besluta om sådana förbud läggs åklagare till. Bakgrunden till förslaget är att endast åklagare skall kunna utfärda yppandeförbud enligt 27 kap. 15 § fjärde stycket RB. Den allmänna motiveringen finns i avsnitt 11.5.3.

27 kap.

1 §
Paragrafen reglerar de grundläggande förutsättningarna för beslag.

I *första stycket* har enbart språkliga ändringar gjorts.

I paragrafens *andra stycke* har, i förtydligande syfte, gjorts ändringar som innebär att beslagsreglerna även omfattar elektroniska upptagningar eftersom dessa svårligen kan inrangeras under begreppet föremål. En elektronisk upptagning kan avse skrift, bilder, musik eller annat som exempelvis programfiler.

I andra meningen i stycket klargörs det att alla särbestämmelser om skriftlig handling i kapitlet skall tillämpas även på elektroniska upptagningar av skrift. Bakgrunden är den tekniska ut-

vecklingen, som har lett till att det i dag är vanligt att skrivelser av allehanda slag tillskapas, bearbetas, tas emot och förvaras i elektronisk form. Elektroniska dokument får således tas i beslag för att säkra innehållet i dessa under samma förutsättningar som gäller för traditionella handlingar. Upptagningen av skrift kan avse text och siffror samt tillhörande bilder eller liknande, dvs. samma innehåll som kan finnas i en traditionell handling. Tillämpningsområdet är i nu aktuellt hänseende inte lika brett som det utvidgade tillämpningsområdet för beslagsregeln i sig, eftersom detta omfattar även exempelvis elektroniska upptagningar av musik och programfiler. Förslaget har utvecklats närmare i avsnitt 11.6.4.

Ändringen innebär att reglerna om beslagsförbud i 2 § blir tillämpliga på elektroniska upptagningar av skrift. Avsikten är inte att utvidga tillämpningsområdet för beslagsförbuden utan enbart att anpassa regleringen till ny teknik. Vidare skall regeln i 12 § om granskning av enskild handling tillämpas på motsvarande information i elektronisk form. Den bestämmelsen är avsedd att begränsa skadan för den enskilde genom att särskilt integritetskänsliga handlingar som t.ex. brev, affärskorrespondens, bokföring och liknande alltid skall granskas snabbt och dessutom endast får granskas av rätten, åklagaren eller annan förundersökningsledare (uppgiften kan dock delegeras i det enskilda fallet).

Det *tredje stycket* är oförändrat.

3 §

I paragrafen regleras beslag av försändelser hos post- och telefordringsföretag.

Första stycket är oförändrat.

Andra stycket är nytt. Där föreskrivs att beslagsregeln skall tillämpas även på elektronisk post. Bakgrunden är att det i 9 a § har införts en möjlighet att kvarhålla elektronisk post. Samma förutsättningar och begränsningar skall gälla för beslag av elektronisk post under befordran som för traditionell post. Motiven till förslaget finns i avsnitt 11.6.2.

9 §

Paragrafen innehåller bestämmelser om kvarhållande av försändelse i avvaktan på beslut enligt 3 § om beslag. Paragrafen har moderniserats språkligt.

I *första stycket* har gjorts den förändringen att en undersökningsledare inte längre kan göra framställning om kvarhållande av försändelse, vilket är en uppgift som åklagare sedan länge har svarat för. Bakgrunden till förslaget har beskrivits i avsnitt 11.6.2.

I *andra stycket* har det gjorts ett tillägg som innebär att kravet på att tiden för kvarhållande inte bestäms längre än vad som är nödvändigt återspeglas i lagtexten. Detta har hittills endast framgått indirekt genom proportionalitetsprincipen. I konsekvens med ändringen i första stycket har vidare förundersökningsledaren bytts ut mot åklagaren.

I *tredje stycket* har, i konsekvens med ändringen i första stycket, föreskrivits att anmälan skall göras till åklagaren.

Det *fjärde stycket* är nytt. Där läggs fast att om det inte längre finns skäl för ett beslut om kvarhållande skall tvångsmedlet omedelbart upphävas. Bestämmelsen har utformats efter mönster av 23 §. För att tvångsmedlet skall kunna upphöra så snabbt som möjligt har inte bara rätten utan även åklagaren getts möjlighet att häva beslut om kvarhållande.

9 a §

I paragrafen, som är ny, regleras kontroll av elektronisk post. Bakgrunden till förslaget har redovisats i avsnitt 11.6.2. Regeln har utformats efter mönster av bestämmelsen i 9 § om kvarhållande av post av traditionellt slag.

I *första stycket* anges förutsättningarna för beslut om kvarhållande. Vid brott med ett års fängelse eller mer i straffskalan (jfr 3 §) kan rätten besluta om kvarhållande av sådana telemeddelanden som väntas komma in till en individualiserad adress för elektronisk post. En förutsättning är dock att inte något beslagsförbud lägger hinder i vägen.

I *andra stycket* finns närmare regler om beslutet. Detta skall gälla för vis tid, högst en månad. Tiden får inte vara längre än vad som är nödvändigt. Till skillnad från vad som gäller i fråga om traditionell post behöver beslutet inte delges. I stället har samma lösning som gäller för hemlig teleavlyssning och hemlig teleövervakning valts, nämligen att rätten i beslutet anger dess varaktighet.

Det *tredje stycket* innehåller hänvisningar till bestämmelserna om kvarhållande av traditionell post. Hänvisningarna innebär dels ett förbud för den som tillhandahåller en allmän kommunikationstjänst mot att underrätta avsändare, mottagare eller annan om åtgärden, dels skyldighet för denna att anmäla till åklagaren när det har kommit in meddelanden. Vidare innebär det att åklagarens skyldighet att omedelbart pröva beslagsfrågan slås fast.

Till *fjärde stycket* har definitionen av vad som är ett telemeddelande (som för närvarande finns i lagen om elektronisk kommunikation) förts över utan någon ändring i sak. Ändringen har kommenterats i avsnitt 11.3.1.

I *femte stycket* föreskrivs en skyldighet att omedelbart häva beslut om kvarhållande om det inte längre finns skäl för åtgärden. Såväl rätten som åklagaren kan häva ett beslut om kvarhållande.

15 §

Paragrafen innehåller dels regler om åtgärder med fast egendom, dels regler om det nya tvångsmedlet förbud mot att rubba elektronisk bevisning.

I *första* och *andra styckena* har enbart språkliga ändringar gjorts.

Det *tredje stycket* är nytt. Det innehåller en regel som gör det möjligt att säkra sådan bevisning i elektronisk form som löper särskild risk att gå förlorad. Denna säkras genom ett föreläggande riktat till den som innehar eller har kontroll över bevisningen. Skälen för förslaget har utvecklats i avsnitt 11.5.1.

Regeln är generell och således tillämplig inte bara på IT-relaterade brott. Däremot gäller den enbart bevisning i elektronisk form. Sådan bevisning kan likaväl förekomma vid våldsbrott

(t.ex. registrerade DNA-uppgifter eller bilder i digital form från en brottsplatsundersökning) som vid förmögenhetsbrott (exempelvis datoriserade uppgifter om värdepapper).

Med uttrycket ”den som innehar” åsyftas inte bara den som fysiskt har informationen i sin dator utan även den som praktiskt förfogar över informationen, t.ex. via terminal, även om den av tekniska skäl är lagrad någon annanstans.

Ett föreläggande om att inte rubba elektronisk bevisning kan riktas mot vem som helst; dock inte mot den som är misstänkt. Föreläggandet, som normalt kommer att utgöra ett förstadium till beslag, får inte heller avse något som inte får tas i beslag.

Endast åklagare får fatta beslut om det nya tvångsmedlet.

Föreläggandet skall vara tidsbegränsat och får inte avse längre tid än vad som är nödvändigt. Den längsta tiden är 90 dagar, men i många fall torde föreläggandet kunna utfärdas för kortare tid. I de fall föreläggandet meddelas som ett led i internationell rättslig hjälp kan det dock vara nödvändigt att utnyttja hela tidsfristen. Det är vidare möjligt att utfärda ett nytt föreläggande innan det gamla har upphört att gälla. Har tiden för föreläggandet löpt ut utan att något beslag eller annan åtgärd för att säkra bevisningen har kommit till stånd upphör automatiskt såväl förbudet att rubba bevisningen som, i förekommande fall, ett yppandeförbud som har meddelats med stöd av fjärde stycket.

Det finns inga formella krav på beslutet. Av skäl som anges i avsnitt 11.5.2 bör den förelagde alltid få en kopia av beslutet, som skall innehålla uppgift om möjligheten att begära rättens prövning.

Även *fjärde stycket* är nytt. Det innehåller en regel som innebär att åklagaren kan förbjuda den som har meddelats ett förbud att rubba elektronisk bevisning att yppa detta. Överträdelse av förbudet bestraffas med stöd av 9 kap. 6 § RB. Den allmänna bakgrunden till förslaget återfinns i avsnitt 11.5.3. Inte heller ett yppandeförbud bör vara längre tid än vad som krävs för att skydda förundersökningen. Av det skälet skall åklagaren alltid ta ställning till om yppandeförbudet kan upphävas när förbudet att

rubba bevisningen upphör genom ett beslag eller annan motsvarande åtgärd.

Det *femte stycket* behandlar möjligheten att få ett rubbandeförbud prövat av rätten. Skälen för förslaget anges i avsnitt 11.5.3. Ett åklagarbeslut kan bringas under domstolsprövning av den mot vilken förbudet har riktats. Om sådan prövning begärs skall reglerna om beslag tillämpas. En förutsättning för att frågan skall kunna prövas är dock att förbudet alltjämt gäller. Har detta ersatts med ett beslag får den drabbade i stället begära prövning av beslaget. Hänvisningen till 6 § innebär att rätten skall hålla förhandling i frågan och att den frist för förhandlingen som anges i 6 § är tillämplig. Rättens beslut skall avse frågan huruvida förbudet skall kvarstå. Rätten kan vid denna prövning inte bara upphäva förbudet utan även inskränka eller ändra detta på annat sätt, t.ex. ändra den tid under vilken uppgifterna skall bevaras orubbade.

En domstol har inte någon rätt att utfärda ett beslut av detta slag. Det innebär att om förbudet har riktats mot fel person kan rätten inte läka detta genom att utfärda ett motsvarande förbud mot någon annan person. Rätten kan inte heller utvidga förbudet till att gälla ytterligare personer.

Om rätten vid prövning av förbudet upphäver detta upphör yppandeförbudet automatiskt.

20 §

I paragrafen anges vilka grundläggande förutsättningar som krävs för beslut om hemlig teleavlyssning eller hemlig teleövervakning. Det *första stycket* är oförändrat.

I *andra stycket* har undantaget för kommunikationsnät av mindre betydelse gjorts snävare. Endast sådana kommunikationsnät som får anses sakna betydelse från allmän kommunikationssynpunkt undantas från tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning. Detta innebär att de mycket lokalt begränsade kommunikationsnät som nämndes när bestämmelsen ursprungligen infördes (t.ex. hörselslingor, porttelefoner och liknande) alltjämt faller utanför tillämpningsområ-

det. Däremot bör inte ett privat telefonnät, även om det är av liten omfattning, falla utanför. Det tidigare uttrycket telenät har bytts ut mot kommunikationsnät, vilket är det uttryck som används numera (bl.a. i lagen om elektronisk kommunikation). Ändringen har kommenterats närmare i avsnitt 11.7.

21 §

Paragrafen innehåller regler om domstols beslut om hemlig teleavlyssning och hemlig teleövervakning. *Första stycket* är oförändrat.

I *andra stycket* har gjorts ett tillägg som innebär att rätten i sitt beslut om hemlig teleavlyssning eller hemlig teleövervakning skall ange om tillståndet omfattar uppgifter som har varit föremål för frysning av elektronisk kommunikation. Förslaget har kommenterats i avsnitt 11.4.4. Eftersom ett beslut om frysning inte innebär någon skyldighet för en operatör att lämna ut uppgifter, utan enbart en skyldighet att bevara uppgifterna (se 6 kap. 21 § andra stycket lagen om elektronisk kommunikation), skall det av domstolens beslut framgå om tillståndet omfattar även dessa uppgifter. Rent praktiskt innebär det att domstolen i förekommande fall förordnar att tillståndet skall gälla från frysningsbeslutet. Om beslutet om frysning av elektronisk kommunikation avser förfluten tid får domstolen ange i beslutet för vilken tid det gäller.

I *tredje stycket* har uttrycket allmänt tillgängliga telenät bytts ut mot motsvarande uttryck som används numera (t.ex. i lagen om elektronisk kommunikation), nämligen allmänna kommunikationsnät.

21 a §

Paragrafen, som är ny, reglerar det nya tvångsmedlet frysning av elektronisk kommunikation.

I *första stycket* anges förutsättningarna för frysning av elektronisk kommunikation. Dessa är dels att det finns rättslig grund för ett beslut om hemlig teleavlyssning eller hemlig teleövervakning (vilket framgår av hänvisningarna till 18 och 19 §§), dels att

det skulle innebära risk att åtgärden skulle gå om intet om man skulle avvakta ett domstolsbeslut. I sådana fall får åklagaren besluta om frysning. Frysningsbeslutet, som gäller omedelbart, innebär att innehållet i de telemeddelanden (vid hemlig teleavlyssning) eller uppgifter om de telemeddelanden (vid hemlig teleövervakning) som utväxlas, eller har utväxlats eftersom beslut om frysning kommer att kunna avse även förfluten tid, skall bevaras i avvaktan på domstolens beslut om hemliga tvångsmedel. Skälen för förslaget har utvecklats i avsnitt 11.4.1. Ett frysningsbeslut innebär enbart att uppgifterna skall bevaras av operatören, inte att han skall röja dem.

Hänvisningen till 21 § innebär att ett åklagarbeslut om frysning skall uppfylla samma formella krav som ett motsvarande beslut av domstol. I beslutet skall således anges vilken teleadress och vilken tid beslutet avser. Eventuella inskränkande villkor bör framgå av beslutet. Vidare måste det framgå om åtgärden får verkställas utanför allmänna kommunikationsnät. Förbudet mot att avlyssna kommunikation mellan den misstänkte och hans försvarare gäller även vid frysning, vilket framgår av hänvisningen till 22 §.

I *andra stycket* regleras åklagarens skyldighet att så snabbt som möjligt underställa domstol frågan om hemlig teleavlyssning eller hemlig teleövervakning. Den allmänna motiveringen finns i avsnitt 11.4.3. Lagen (1930:173) om beräkning av lagstadgad tid är tillämplig på fristen. Om åklagaren inte ger in en framställning till domstol om användning av hemliga tvångsmedel skall han genast häva frysningen. I ett sådant fall kommer den information som har samlats in med anledning av frysningsbeslutet aldrig att bli tillgänglig.

Domstolens handläggning regleras i *tredje stycket*. Där anges en frist för när rätten skall hållas förhandling. Förslaget utvecklas närmare i avsnitt 11.4.4.

28 kap.

1 a §

Paragrafen, som behandlar husrannsakan i IT-miljö, är ny. Den allmänna motiveringen finns i avsnitt 11.6.3.

Det *första stycket* har utformats efter mönster av 1 §. Regleringen skiljer sig dock i två avseenden. Det ena är att bestämmelsen inte anger någon rumslig begränsning. Eftersom straffprocessuella tvångsmedel är territoriellt begränsade ligger det dock i sakens natur att åtgärden endast kan avse datorer, datorsystem och annan liknande utrustning som finns i Sverige.

Den andra skillnaden är att syftet med åtgärden skall vara att söka efter data i elektronisk form. Detta skall jämföras med att det i 1 § anges att det som skall eftersökas skall vara föremål. Om det krävs undersökning av en dator eller ett datorsystem av annat skäl än att eftersöka elektroniska data skall därför i stället 1 § tillämpas.

Ändamålen med husrannsakan i IT-miljö är desamma som för husrannsakan i traditionell miljö, nämligen att åtgärden skall syfta till beslag eller till att utröna omständighet av betydelse för utredningen om brottet. Proportionalitetsprincipen (3 a §) skall tillämpas vid beslut om husrannsakan i IT-miljö.

Det som kan bli föremål för husrannsakan är för det första datorsystem eller delar därav (t.ex. en hårddisk eller en server). För det andra är det fråga om persondatorer och andra typer av datorer samt alla typer av utrustning som hör till dessa. För att markera att även andra föremål som är utrustade med datoriserade funktioner och som innehåller data i elektronisk form som kan ha betydelse för en brottsutredning omfattas av bestämmelsens tillämpningsområde har uttrycket ”annan liknande teknisk utrustning” använts. Härigenom kommer t.ex. en modern mobiltelefon eller GPS-utrustning i en taxibil att kunna undersökas med stöd av bestämmelsen. Till annan liknande utrustning räknas även fysiska föremål på vilka information i elektronisk form kan lagras, t.ex. disketter och CD.

I *andra stycket* regleras husrannsakan hos annan än den som är misstänkt. För husrannsakan hos målsägande eller tredje man ställs samma grundläggande krav som i fråga om husrannsakan enligt 1 §. Härutöver krävs det att det finns konkreta skäl att tro att åtgärden skall leda till resultat på grund av att brottet har förövats där utrustningen finns, att den misstänkte har gripits där eller att det av något annat skäl finns synnerlig anledning att anta att husrannsakan skall leda fram till beslag eller till annan utredning om brottet.

Stycket innehåller även en regel om samtycke till husrannsakan. Möjligheten att genomföra husrannsakan med samtycke gäller bara för icke misstänkta personer. Samtycke innebär att kravet på att åtgärden skall förväntas leda till visst resultat inte behöver vara uppfyllt, medan det även i dessa fall krävs att det finns misstanke om ett konkret brott med fängelse i straffskalan.

Enligt *tredje stycket* får en husrannsakan enligt denna paragraf verkställas via ett kommunikationsnät. Som krav uppställs att det finns särskilda skäl för sådan verkställighet. Ett särskilt skäl kan vara att den hos vilken husrannsakan skall göras föredrar den formen av verkställighet och frivilligt medverkar för att underlätta att den genomförs, exempelvis genom att tillhandahålla åtkomstkoder eller lösenord. Ett annat skäl kan vara att åtgärden är mycket brådskande, att det krävs särskild teknisk expertis för att genomföra åtgärden samt att sådan expertis inte tillräckligt snabbt kan ta sig till den plats där husrannsakan annars skulle äga rum. Resursbrist kan dock inte i sig utgöra särskilda skäl.

I fråga om verkställighet av husrannsakan i IT-miljö gäller detsamma som för husrannsakan i allmänhet. Detta innebär först och främst att proportionalitetsprincipen (3 a §) skall tillämpas även vid verkställigheten. Andra begränsningar, t.ex. i fråga om användning av våld (6 §) skall också iakttas. Vidare ställs samma krav i fråga om dokumentation (9 §), vittne och underrättelser (7 §) m.m. Det som påträffas får granskas endast under de förutsättningar som anges i 8 §. Vid verkställighet via nät har dock undantag gjorts från regeln om att husrannsakan mellan klockan

nio på kvällen och sex på morgonen kräver särskilda skäl (se kommentaren till ändringarna i 6 §).

Reglerna om behörighet att besluta om husrannsakan enligt den nya bestämmelsen finns i 4 och 5 §§.

4 §

Paragrafen innehåller regler om vem som får besluta om husrannsakan.

Enligt *första stycket* får sådan husrannsakan i IT-miljö som verkställs där datorn eller datorsystemet finns beslutas av rätten, åklagare eller annan förundersökningsledare. Rätten skall enligt huvudregeln besluta om husrannsakan via kommunikationsnät, eftersom en sådan åtgärd har stora likheter med hemliga tvångsmedel på teleområdet. Detta har utvecklats närmare i avsnitt 11.6.3. Finns det samtycke får dock åklagare besluta om åtgärden. Som framgått av kommentaren till 1 a § får husrannsakan via nät inte användas mot den som är misstänkt.

Andra och *tredje styckena* är oförändrade.

5 §

En polisman får enligt nuvarande regler besluta om husrannsakan vid fara i dröjsmål, med undantag för husrannsakan för delgivning. En motsvarande inskränkning skall gälla för beslut om husrannsakan i IT-miljö, vilket utvecklas närmare i avsnitt 11.6.3. Av det skälet har husrannsakan enligt 1 a § undantagits från paragrafens tillämpningsområde.

6 §

Paragrafen innehåller regler om verkställighet av husrannsakan. I *första* och *andra styckena* har enbart språkliga moderniseringar gjorts.

I det *tredje stycket* har undantag från regeln om att verkställighet nattetid bör undvikas gjorts för sådan husrannsakan som verkställs via kommunikationsnät. Skälen för detta har utvecklats i avsnitt 11.6.3.

7 §

I paragrafen regleras närvaro vid husrannsakan och underrättelse om åtgärden. I *första, andra* och *tredje styckena* har språket moderniserats, men i sak är bestämmelserna oförändrade. Det ålderdomliga uttrycket hemmavarande husfolk har bytts ut mot den mer neutrala termen hemmavarande. Till denna kategori räknas bl.a. familjemedlemmar, sammanboende, personer som är anställda i hushållet och andra som på likartat sätt har en personlig anknytning till den som utsätts för åtgärden.

Det *fjärde stycket* är nytt. Möjligheten att verkställa husrannsakan via elektroniska kommunikationsnät innebär att paragrafen måste anpassas. De enda bestämmelser som skall tillämpas på en sådan husrannsakan är dels regeln om att förrättningsmannen får anlita biträde av sakkunnig eller annan, dels regeln om underrättelseskyldighet mot den som har utsatts för åtgärden.

38 kap.

2 §

Paragrafen reglerar editionsskyldighet. *Första, andra* och *tredje styckena* har endast moderniserats språkligt.

I ett nytt *fjärde stycke* har, i konsekvens med ändringen i 27 kap. 1 §, i förtydligande syfte lagts till att vad som föreskrivs om skriftlig handling även gäller för elektronisk upptagning av skrift. Genom placeringen i 2 § har markerats att bestämmelsen skall tillämpas på editionsskyldigheten som sådan samt på de regler som gäller för edition, men däremot inte på 1 §. Ändringen har kommenterats i avsnitt 11.6.4.

39 kap.

5 §

Paragrafen innehåller regler om syn. Ändringarna är av samma slag som i 38 kap. 2 §.

12.2 Förslaget till ändring i lagen med särskilda bestämmelser om tvångsmedel i vissa brottmål

5 §

I *första stycket* har reglerna om frysning av elektronisk kommunikation gjorts tillämpliga på de brott som behandlas i lagen. Frysning kan beslutas vid dessa brott i samma utsträckning som hemlig teleavlyssning respektive hemlig teleövervakning. Ändringen har kommenterats i avsnitt 11.10.2.

Som en konsekvens av denna ändring har *andra stycket* ändrats på det sättet att åklagares rätt att interimistiskt besluta om hemlig teleavlyssning och hemlig teleövervakning har tagits bort. Reglerna om frysning av elektronisk kommunikation är generellt tillämpliga, varför det inte längre finns något behov av interimistiska beslut om hemlig teleavlyssning och hemlig teleövervakning. Däremot kommer åklagare även i fortsättningen att ha möjlighet att intermistiskt besluta om hemlig kameraövervakning.

12.3 Förslaget till ändringar i brottsbalken

4 kap.

9 c §

Paragrafen behandlar straffansvar för intrång i och påverkan på datorsystem och datainformation.

Straffansvaret har utvidgats att omfatta även olovlig avlyssning av signaler från datorer och datorsystem. Den allmänna motiveringen finns i avsnitt 11.1.3. Bestämmelsen är subsidiär till regeln om brytande av telehemlighet. Tillämpningsområdet för den bestämmelsen ändras inte. Avlyssning som har formen av direkt intrång är också redan straffbar. Den nya straffbestämmelsen ger däremot skydd mot andra former av avlyssning, framför allt avlyssning av elektromagnetiska emissioner.

I likhet med vad som gäller för olovlig avlyssning av samtal straffbeläggs endast avlyssning med tekniska hjälpmedel.

Avlyssningen kan avse såväl elektromagnetiska emissioner som andra signaler, men det straffbara området omfattar endast sådana signaler som inte är allmänt tillgängliga. Härigenom kommer straffansvaret inte att omfatta t.ex. radiosändningar som riktar sig till allmänheten.

Gärningen skall ha begåtts olovligen, vilket bl.a. innebär att t.ex. den som för ägarens/brukarens räkning testar systemets säkerhet mot avlyssning inte kan straffas för åtgärden.

Gärningsmannen skall ha haft för avsikt att genom avlyssningen få del av information. Däremot behöver gärningsmannen inte faktiskt ha tagit del av den information som har avlyssnats utan det räcker att den har blivit tillgänglig för honom. Det spelar således inte heller någon roll om informationen har varit helt utan värde för gärningsmannen, t.ex. därför att den har haft en form eller varit på ett språk som han inte har kunnat tillgodogöra sig.

Uttrycket automatisk databehandling har bytts ut mot det uttryck som används numera, nämligen automatiserad databehandling.

9 d §

Paragrafen är ny. Den innehåller en bestämmelse om förberedelse till dataintrång i form av olovlig avlyssning. Paragrafen har utformats efter mönster av 9 b § men getts en modernare språklig utformning. Den allmänna motiveringen finns i avsnitt 11.1.3.

14 kap.

9 §

I *första stycket* har endast några språkliga justeringar gjorts för att modernisera paragrafen.

Andra stycket är nytt. Det kommenteras närmare i avsnitt 11.1.4.

Genom ändringen utvidgas ansvaret för brukande av falsk urkund till att omfatta även elektroniska dokument. Den som åberopar en icke autentisk sammanställning av elektroniska data kan

dömas för brukande av falsk urkund, även om sammanställningen i sig, på grund av sin elektroniska form, inte uppfyller de i kapitlet angivna kraven på att vara urkund. Den måste dock, vilket följer av kravet på att det är en sammanställning, ha ett urskiljbart innehåll och i övriga hänseenden vara jämförbar med en urkund bl.a. genom att den innehåller en tydlig utställare.

Begreppet data i elektronisk form finns redan dels i lagen om kvalificerade elektroniska signaturer, dels i 5 kap. 3 § i sekretesslagen. Med data i elektronisk form avses här detsamma som i dessa lagar.

Sammanställningen kan omfatta text, siffror, bilder eller annat. Det krävs att den är i elektronisk form, men formen kan i sig variera. Det kan t.ex. vara fråga om text som biläggs elektronisk post eller en ekonomisk sammanställning i form av en datafil.

För straffansvar krävs att sammanställningen antingen i sin helhet är ett falsarium eller att en äkta sammanställning har påverkats. Sammanställningen kan vara icke autentisk t.ex. på det sättet att den ger sken av att härröra från en annan utställare än den verkliga. Vidare kan sammanställningen ha påverkats på det sättet att den har tillförts eller fråntagits uppgifter som gör att den inte längre är autentisk.

Blotta användningen av en icke autentisk sammanställning är emellertid inte tillräcklig. Härutöver krävs det att den som åberopar sammanställningen ger sken av att den är autentisk. Därigenom undantas från det straffbara området användning där det direkt eller av sammanhanget framgår från att uppgifterna härrör från någon annan än utställaren. Ytterligare ett krav som skall uppfyllas är att åtgärden skall innebära fara i bevishänseende. Därmed utesluts gärningar där det inte finns någon risk att sammanställningen skall betraktas som autentisk t.ex. på grund av att en viss text används i en satir.

Bestämmelsen är inte avsedd att användas om gärningen kan bestraffas som förfalskning, t.ex. om en elektronisk urkund har en sådan utställarangivelse att ansvar för urkundsförfalskning kan utkrävas.

12.4 Förslaget till ändring i sekretesslagen

16 kap.

1 §

Ändringen, som har kommenterats närmare i avsnitt 11.8.1, har sin grund i att det införs nya tvångsmedel i rättegångsbalken.

Sekretessen i 5 kap. 1 § sekretesslagen, som skyddar brottsutredningar och annan brottsbekämpande verksamhet, innebär få begränsningar i meddelarfriheten. De begränsningar som finns rör uppgifter om hemliga tvångsmedel, dvs. tvångsmedel som verkställs utan den misstänktes vetskap. För närvarande är meddelarfriheten begränsad i fråga om uppgifter om hemlig teleavlyssning, hemlig teleövervakning, kvarhållande av försändelse samt hemlig kameraövervakning.

Beslut om frysning av elektronisk kommunikation skall utgöra ett kort förstadium till domstols beslut om hemlig teleavlyssning eller hemlig teleövervakning. Tvångsmedlet är till sin karaktär sådant att det, för att kunna fungera på avsett sätt, måste hållas hemligt för den misstänkte. Samma begränsningar i meddelarfriheten som gäller för andra hemliga tvångsmedel skall gälla för frysning av elektronisk kommunikation.

I paragrafen görs också en hänvisning till 27 kap. 9 a § RB. Härigenom kommer uppgifter om kvarhållande för eventuellt beslag av elektronisk post att omfattas av begränsningarna i meddelarfriheten, på samma sätt som nu är fallet med uppgifter om kvarhållande av traditionell post.

12.5 Förslaget till ändring i lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

28 §

Paragrafen innehåller undantag från reglerna i bl.a. 27 kap. RB om vem som fattar beslut i fråga om hemliga tvångsmedel.

I *första stycket* har åklagares rätt att interimistiskt besluta om hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. RB upphävts. Bakgrunden till detta är att reglerna om frysning av elektronisk kommunikation är generellt tillämpliga. Det finns då inte något behov av interimistiska beslut.

Vidare har, i fråga om kvarhållande av försändelse, föreskrivits att åklagare får besluta interimistiskt i fråga om kvarhållande av elektronisk post.

Hänvisningarna till rättegångsbalken har anpassats till de nya reglerna.

I *andra stycket* har gjorts en hänvisning till reglerna om frysning av elektronisk kommunikation beträffande skyldigheten att underställa domstol frågan om tvångsmedelsanvändning. Det innebär att beslut om hemlig kameraövervakning och om kvarhållande av försändelse skall anmälas genast, medan samma regler gäller för underställande av beslut om frysning enligt den nu aktuella lagen som enligt rättegångsbalken.

Ändringarna har kommenterats närmare i avsnitt 11.10.3.

12.6 Förslaget till ändringar i lagen om internationell rättslig hjälp i brottmål

Ändringarna utgör främst följdändringar med anledning av ändrade regler om tvångsmedel i 27 och 28 kap. RB. För att de nya tvångsåtgärderna skall kunna användas vid internationellt samarbete för att underlätta brottsutredning och process i en annan stat måste nya bestämmelser införas i lagen om internationell rättslig hjälp. Vidare har nya regler om säkrande och röjande av trafikuppgifter införts.

1 kap.

2 §

Bakgrunden till ändringarna har tecknats i avsnitt 11.9.1.

Ändringarna innebär att uppräkningen i *första stycket*, som bl.a. uttömmande anger med vilka tvångsmedel som Sverige lämnar rättslig hjälp, kompletteras. Det nya tvångsmedlet frysning av elektronisk kommunikation läggs till i punkten 7, som reglerar hemlig teleavlyssning och hemlig teleövervakning. I punkt 5, som rör bl.a. husrannsakan och beslag, görs ett tillägg som innebär att förbud mot rubbande av bevisning i elektronisk form ingår bland de uppräknade tvångsmedlen. Vidare införs två nya punkter, 6 och 9. Punkt 6 reglerar kvarhållande av försändelse (27 kap. 9 § RB) och kvarhållande av elektronisk post (27 kap. 9 a § RB). Punkt 9 behandlar röjande av trafikuppgifter.

Andra och *tredje styckena* är oförändrade.

2 kap.

1 §

Ändringarna består enbart i följdändringar med anledning av att nya åtgärder räknas upp i 1 kap. 2 §. I *första* och *andra styckena* har därför hänvisningarna till punkter i nämnda paragraf justerats. *Tredje stycket* är oförändrat.

2 §

Ändringarna i fråga om hänvisningar till 1 kap. 2 § är av samma slag som i föregående paragraf.

I andra meningen anges i vilka fall det krävs dubbel straffbarhet för rättslig hjälp. Ett sådant krav uppställs för hjälp med de nya åtgärderna, med undantag för hjälp med röjande av trafikuppgifter. Kravet på dubbel straffbarhet är dock uppmjukat när det gäller rubbande av bevisning i elektronisk form, i samma utsträckning som för beslag. I hänvisningen till 4 kap. 20 § har därför förbud mot rubbande av bevisning i elektronisk form lagts till, samtidigt som en motsvarande ändring har gjorts i den paragrafen.

Ändringen har kommenterats i avsnitt 11.9.1.

4 §
Första stycket är oförändrat.

Med anledning av att två nya paragrafer (22 a och 28 a §§), som bl.a. behandlar vad en ansökan om rättslig hjälp bör innehålla, har införts i 4 kap. har hänvisningen i *andra stycket* kompletterats. Ändringen har kommenterats i avsnitt 11.9.2.

Även *tredje stycket* är oförändrat.

3 kap.

1 §
I paragrafen anges vilka bestämmelser om innehållet i ansökan m.m. som svenska myndigheter skall iaktta när de begär rättslig hjälp utomlands. Det *första stycket* är oförändrat. I *andra stycket* har hänvisningar till de nya bestämmelserna i 4 kap. gjorts. Ändringen har kommenterats i avsnitt 11.9.3.

4 kap.

Rubrikerna

Rubriken före 18 § har ändrats för att markera att avsnittet behandlar andra åtgärder i 27 kap. RB än enbart beslag. I rubriken före 25 § har m.m. lagts till eftersom avsnittet omfattar även frysning av elektronisk kommunikation. Nya rubriker har införts före de nya paragraferna 26 a, 26 d och 28 a §§.

18 §
I paragrafen har gjorts en hänvisning som innebär att åtgärder enligt 27 kap. RB skall handläggas av åklagare. Detta gäller dock inte i fråga om beslag, som behandlas i 16 §. Bakgrunden till ändringen är dels de nya reglerna om förbud mot rubbande av elektronisk bevisning och frysning av elektronisk kommunikation, dels att kvarhållande av försändelse har räknats upp bland de

tvångsmedel som får användas på begäran av annan stat. Nu nämnda tvångsåtgärder hanteras av åklagare.

20 §

I paragrafen behandlas undantag från kravet på dubbel straffbarhet för vissa tvångsmedel.

För husrannsakan och beslag gäller enligt *första stycket* lägre krav i förhållande till de övriga nordiska länderna och medlemmarna i den Europeiska unionen. En motsvarande uppmjukning görs i fråga om rubbande av bevisning i elektronisk form, eftersom detta tvångsmedel är tänkt som ett förstadium till beslag. Det kan då inte ställas högre krav än som gäller för beslag i motsvarande fall. Förslaget har kommenterats i avsnitt 11.9.1.

Andra stycket är oförändrat.

25 §

Paragrafen reglerar förfarandet vid hemlig teleavlyssning eller hemlig teleövervakning på begäran av annan stat. *Första stycket* är oförändrat.

I *andra stycket*, som är nytt, görs undantag från regeln i 27 kap. 24 § RB om omedelbart granskning av material från hemlig teleavlyssning och förstörande av visst material. Ändringen har motiverats i avsnitt 11.9.2.

26 a §

Paragrafen är ny. Förslaget har utvecklats i avsnitt 11.9.2.

Det *första stycket* reglerar vad som gäller i de fall där en annan stat begär brådskande hjälp med uppgifter som kan säkras med stöd av reglerna om frysning av elektronisk kommunikation. En åklagare skall omedelbart ta ställning till framställningen och, om förutsättningarna är uppfyllda, besluta i frågan. Ett beslut om frysning av elektronisk kommunikation skall därefter underställas rättens prövning inom några få dagar, varför det i andra stycket, genom hänvisningen till 25 §, föreskrivs att ansökan om hjälp med frysning skall behandlas som om det vore en ansökan om hjälp med hemlig teleavlyssning eller hemlig teleövervakning.

Om rätten meddelar beslut om hemlig teleavlyssning eller hemlig teleövervakning skall reglerna i 25 § andra stycket (om undantag från skyndsam granskning och förstörande av material från hemlig teleavlyssning), i 26 b § (om den fortsatta handläggningen av ansökan) och 26 c § (om åklagarens skyldighet att i visst fall omedelbart underrätta den andra staten om vad som har kommit fram) tillämpas.

Om de begärda uppgifterna i stället kan inhämtas med stöd av 6 kap. 22 § första stycket punkt 4 lagen om elektronisk kommunikation skall åklagaren bistå med detta (se kommentaren till 28 a §).

I *andra stycket* regleras den fortsatta handläggningen när åklagaren har beslutat om frysning av elektronisk kommunikation. Framställningen om frysning skall då, som nyss har nämnts, betraktas som en framställning om hemlig teleavlyssning eller hemlig teleövervakning.

26 b §

Paragrafen, som är ny, innehåller i *första stycket* bestämmelser om det fortsatta förfarandet när en annan stat har begärt skyndsam hjälp med frysning eller annat säkrande.

Oavsett vilken åtgärd som vidtas med anledning av framställningen skall den begärande staten följa upp denna med en ny framställning om att de inhämtade uppgifterna lämnas över, om det inte redan av den ursprungliga framställningen framgår att den avser såväl säkrande som överlämnande. Den allmänna motiveringen finns i avsnitt 11.9.2. Den andra staten måste begära att få materialet inom sextio dagar. Om så inte är fallet skall uppgifterna omedelbart förstöras.

Det ankommer på åklagaren att se till att den andra staten hålls underrättad om tidsfristen, att bevaka att den hålls samt att se till att materialet förstörs om ansökan om att få ut materialet inte kommer in i rätt tid eller om materialet inte skall lämnas ut av något annat skäl.

Om ansökan görs i rätt tid och på rätt sätt skall åklagaren ta ställning till om materialet (eller enbart en del av det) skall över-

lämnas till den andra staten. Det generella kravet i 2 kap. 10 § på skyndsam handläggning av framställningar om rättslig hjälp skall tillämpas.

I *andra* stycket regleras den situationen att den begärande staten redan i sin grundläggande ansökan om hjälp har begärt både att uppgifter skall säkras och att de skall lämnas över. I sådant fall skall uppgifterna lämnas över så snart de har samlats in och åklagaren har hunnit pröva begäran om överlämnande.

26 c §

Paragrafen är ny. I den regleras skyldigheten att underrätta den begärande staten om vissa trafikuppgifter. Bakgrunden är att säkrandet av trafikuppgifter i vissa fall kan ha formen av frysning, hemlig teleövervakning eller hemlig teleavlyssning. Den allmänna motiveringen finns i avsnitt 11.9.2.

26 d §

Paragrafen är ny. Regleringen i lagen bygger på att svenska åklagare skall kunna ansöka om rättslig hjälp med åtgärder av samma slag som Sverige lämnar hjälp med. Konventionen om IT-relaterad brottslighet kommer sannolikt att få stor betydelse för det internationella samarbetet på några speciella områden. Om ett land lämnar rättslig hjälp med interimistiska åtgärder som förstadium till åtgärder som motsvarar hemlig teleavlyssning och hemlig teleövervakning, eller med säkrande av trafikuppgifter i någon annan form, skall en svensk åklagare kunna begära sådan hjälp. Bakgrunden till förslaget har tecknats i avsnitt 11.9.3.

28 a §

Paragrafen är ny. I *första stycket* regleras förfarandet vid säkrande och röjande av lagrade trafikuppgifter. I ansökan om säkrande skall det framgå vilket eller vilka telemeddelanden som åtgärden gäller. Åklagaren skall genast pröva framställningen. Vid den prövningen får åklagaren bedöma om det är fråga om uppgifter som kan hämtas in med stöd av 6 kap. 22 § första stycket punkt 4 lagen om elektronisk kommunikation eller om det i stället

krävs beslut om hemlig teleövervakning för förfluten tid. I det senare fallet aktualiseras frågan om eventuell frysning av elektronisk kommunikation (27 kap. 21 a § RB), vilket åklagaren själv kan besluta om. Man torde kunna utgå från att ansökan om säkrande i ett sådant fall också innehåller de uppgifter som krävs enligt 28 a §. För förfarandet när uppgifter har säkrats gäller reglerna i 26 b §, vilket innebär att den begärande staten skall följa upp en framställning som enbart avser säkrande med en framställning om att uppgifterna skall röjas.

I *andra* stycket regleras vad åklagaren skall göra om det i samband med säkrandet av trafikuppgifter upptäcks att en tjänsteleverantör i ett tredje land har medverkat i överföringen av det eller de telemeddelanden som framställningen avser. Åklagaren skall då snabbt underrätta den begärande staten om detta och samtidigt lämna tillräckliga uppgifter för att tjänsteleverantören skall kunna identifieras och att meddelandets väg skall kunna spåras.

12.7 Förslaget till ändringar i lagen om elektronisk kommunikation

Ändringarna har sin grund bl.a. i att det i rättegångsbalken införs ett nytt tvångsmedel som förstadium till de hemliga tvångsmedlen på teleområdet, nämligen frysning av elektronisk kommunikation. Vidare införs kvarhållande av elektronisk post. Detta kräver följdändringar i lagen om elektronisk kommunikation eftersom operatörerna har en viktig roll vid verkställandet av dessa tvångsmedel. Operatörernas skyldighet att avslöja trafikuppgifter utvidgas också.

6 kap.

1 §
Första och *andra* styckena är oförändrade.

Det *tredje stycket* är nytt. Definitionen av vad som är ett telemeddelande har förts över från lagen om elektronisk kommunikation till rättegångsbalken, där det sakligt sett hör hemma (se avsnitt 11.3.1). Eftersom uttrycket används i vissa paragrafer i kapitlet (19 § andra stycket och 23 §) klargörs det att definitionen alltjämt gäller för kapitlet.

8 §

I paragrafen regleras i tre punkter vilka undantag som gäller från kravet på att trafikuppgifter snabbt skall utplånas eller avidentifieras. Punkterna 1 och 3 är oförändrade. I punkt 2 har ett tillägg gjorts. Detta innebär att undantaget gäller för uppgifter som omfattas av beslut om frysning av elektronisk kommunikation samt för uppgifter om kvarhållande av elektronisk post.

19 §

Paragrafen behandlar operatörers anpassningsskyldighet. I *första stycket* har i uppräkningen av tvångsmedel tagits med dels det nya tvångsmedlet frysning av elektronisk kommunikation, dels kontroll av elektronisk post.

Andra stycket är oförändrat. Det kommer emellertid att omfatta även telemeddelanden som har kvarhållits med stöd av 27 kap. 9 a § RB.

Det *tredje stycket*, som innehållit definitionen av vad som är ett telemeddelande, har upphävts eftersom definitionen inte längre sakligt hör hemma i lagen om elektronisk kommunikation. Definitionen har i sak oförändrad flyttats över till 27 kap. 9 a § RB.

Även *fjärde stycket* är oförändrat.

21 §

I *första stycket* har operatörernas tystnadsplikt utökats till att omfatta även frysning av elektronisk kommunikation genom tillägget av en ny tredje punkt. Förslaget har kommenterats i avsnitt 11.8.2. Tystnadsplikten omfattar för närvarande beslut att kvarhålla försändelse enligt 27 kap. 9 § RB. Genom en hänvis-

ning till 27 kap. 9 a § görs klart att tystnadsplikten även avser kvarhållande av elektronisk post.

Andra stycket är nytt. Det innehåller en föreskrift om att uppgifter som har bevarats med anledning av ett beslut om frysning av elektronisk kommunikation inte får lämnas ut innan det finns ett domstolsbeslut om hemlig teleavlyssning eller hemlig teleövervakning. Bakgrunden till förslaget har tecknats i avsnitt 11.4.1. Vidare har erinrats om att skyldigheten att lämna trafikuppgifter om särskilt utpekade meddelanden regleras särskilt (22 § första stycket 4). Om sådana uppgifter ingår bland de uppgifter som har bevarats kan de således lämnas ut utan hinder av vad som föreskrivs i första meningen.

22 §

I f*örsta stycket,* som reglerar operatörers skyldighet att utan hinder av tystnadsplikten lämna vissa uppgifter till myndigheter, har gjorts ett tillägg i punkt 3. Tillägget klargör att denna bestämmelse inte skall tillämpas på uppgifter som härrör från frysning av elektronisk kommunikation.

En ny punkt 4 har införts. I denna regleras skyldigheten att röja trafikuppgifter. Förslaget har kommenterats i avsnitt 11.8.3. Det ställs fyra konkreta krav för att bestämmelsen skall vara tillämplig. Det skall finnas misstanke om ett konkret brott och fängelse ett år skall kunna följa på brottet. Vidare skall trafikuppgifterna som efterfrågas gälla ett eller flera specificerade telemeddelanden. Den som begär uppgifter skall kunna ange vilket meddelande saken rör. Skyldigheten att lämna uppgifter är alltså inte generell. Vidare skall det vara fråga om lagrade uppgifter, vilket innebär att förfrågan inte får avse framtida uppgifter. Det tredje kravet är att uppgiften behövs för att identifiera tjänsteleverantörerna och meddelandets väg. Alla uppgifter som kan belysa den frågan skall lämnas. Slutligen är det endast åklagare eller polismyndighet som har rätt att få uppgifter.

Genom att en ny fjärde punkt har skjutits in har punkterna 4 till 8 numrerats om.

I *andra stycket* har hänvisningen till den tidigare punkten 8 ändrats, till följd av omnumreringen i föregående stycke. I övrigt är stycket oförändrat.

Bilaga 1 Konvention om IT-relaterad brottslighet (ETS 185)

Preliminär översättning

Budapest den 23 november 2001

Ingress

Medlemsstaterna i Europarådet och de övriga stater som har undertecknat denna konvention,

som beaktar att Europarådets syfte är att skapa en fastare enhet mellan dess medlemmar,

som erkänner värdet av att främja samarbete med de övriga stater som är parter i denna konvention,

som är övertygade om nödvändigheten av att, som en prioriterad fråga, driva en gemensam straffrättslig politik som syftar till att skydda samhället mot IT-relaterad brottslighet, bl.a. genom att anta lämplig lagstiftning och främja internationellt samarbete,

som är medvetna om de djupgående förändringar som har föranletts av digitalisering, konvergens och fortgående globalisering av datornät,

som är oroade över faran för att datornät och elektroniska uppgifter också kan användas för att begå brott och att bevisning om sådana brott kan lagras och överföras genom dessa datornät,

som erkänner behovet av samarbete mellan staterna och det privata näringslivet i att bekämpa IT-relaterad brottslighet och behovet av att skydda rättmätiga intressen beträffande användning och utveckling av informationsteknologier,

som anser att en effektiv kamp mot IT-relaterad brottslighet fordrar ett utvidgat, snabbt och väl fungerande internationellt samarbete i straffrättsliga frågor,

som är övertygade om att denna konvention behövs för att avskräcka från gärningar som riktar sig mot datorsystemens, datornätens och de datorbehandlingsbara uppgifternas förtrolighet, integritet och tillgänglighet, liksom från missbruk av dessa system, nät och uppgifter genom att föreskriva att sådana gärningar kriminaliseras så som det beskrivs i konventionen, och att befogenheter som är tillräckliga för att effektivt bekämpa dessa brott införs, genom att underlätta upptäckt, utredning och lagföring av dem, både på det nationella och det internationella planet och genom att sörja för system för ett snabbt och pålitligt internationellt samarbete,

som är medvetna om behovet av att säkerställa en lämplig avvägning mellan intresset av att lag och ordning upprätthålls och respekten för de grundläggande mänskliga rättigheterna så som de garanteras i 1950 års Europarådskonvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna, 1966 års FN-konvention om medborgerliga och politiska rättigheter och andra tillämpliga internationella fördrag om mänskliga rättigheter, som bekräftar allas rätt att utan inblandning hysa åsikter liksom rätten till yttrandefrihet, innefattande frihet att söka, ta emot och sprida information och idéer av alla slag, oberoende av gränser, samt rätten till respekt för privatlivet,

som också är medvetna om rätten till skydd för personuppgifter, såsom denna rätt tillgodoses exempelvis i 1981 års Europarådskonvention om skydd för enskilda vid automatisk databehandling av personuppgifter,

som beaktar 1989 års FN-konvention om barnets rättigheter och 1999 års ILO-konvention mot de värsta formerna av barnarbete,

som beaktar de Europarådskonventioner som finns om samarbete på det straffrättsliga området liksom liknande fördrag mellan Europarådets medlemsstater och andra stater och som understryker att den nu aktuella konventionen är avsedd att komplettera dessa konventioner för att effektivisera brottsutredningar och rättegångar om brott relaterade till datorsystem och datorbehandlingsbara uppgifter samt möjliggöra insamling av bevis i elektronisk form om brott,

som välkomnar den senaste utvecklingen som ytterligare främjar internationell förståelse och internationellt samarbete i att bekämpa IT-relaterad brottslighet, innefattande åtgärder vidtagna av Förenta nationerna, OECD, Europeiska unionen och G8,

som erinrar om ministerkommitténs rekommendationer nr R (85)10 om praktisk tillämpning av Europeiska konventionen om inbördes rättshjälp i brottmål avseende bevisinsamling vid avlyssning av teleförbindelser, nr R (88)2 om piratverksamhet avseende upphovsrätt och närstående rättigheter, nr R (87)15, som reglerar användningen av personuppgifter i polisiär verksamhet, nr R (95)4 om skydd för personuppgifter inom telekommunikationstjänster med särskild hänvisning till telefoni samt nr R (89)9 om datorrelaterade brott, som ger riktlinjer för nationella lagstiftande församlingar om definition av vissa datorbrott och nr R (95)13 om problem inom straffprocessrätten som hör samman med informationsteknologi,

som beaktar resolution nr 1, antagen av de europeiska justitieministrarna vid deras tjugoförsta konferens i Prag den 10-11 juni 1997, vilken rekommenderar ministerkommittén att stödja det arbete om IT-brottslighet som utförs av Europarådets kommitté för brottsfrågor för att tillnärma olika länders nationella straffrättsliga bestämmelser och möjliggöra användning av effektiva utredningsmetoder i fråga om sådana brott, liksom resolution nr 3, antagen vid de europeiska justitieministrarnas tjugotredje konferens i London den 8-9 juni 2000, vilken uppmanar de förhandlande parterna att fortsätta sina ansträngningar med sikte på att finna lämpliga lösningar för att göra det möjligt för största möjliga antal stater att bli parter i konventionen och erkänner behovet av ett snabbt och effektivt system för internationellt samarbete, vari vederbörligen beaktas de särskilda krav som ställs i kampen mot IT-relaterad brottslighet,

som även beaktar den handlingsplan som antogs av Europarådets stats- och regeringschefer vid deras andra toppmöte i Strasbourg den 10-11 oktober 1997 för att söka gemensamma svar på utvecklingen av nya informationsteknologier, som grundar sig på Europarådets normer och värderingar,

har kommit överens om följande.

Kapitel I Användning av termer

Artikel 1 Definitioner

I denna konvention används följande definitioner:

a) *datorsystem*: en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatiserad behandling av uppgifter.

b) *datorbehandlingsbara uppgifter*: framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett datorsystem, inklusive program som utformats för att få ett datorsystem att utföra en viss funktion.

c) *tjänsteleverantör*:

i) en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och

ii) varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst.

d) *trafikuppgifter*: datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av ett datorsystem, vilka alstrats av ett datorsystem som ingick i kommunikationskedjan och anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst.

Kapitel II Åtgärder som skall vidtas på nationell nivå

Avsnitt 1 Materiell straffrätt

Avdelning 1 Brott mot datorbehandlingsbara uppgifters och datorsystems förtrolighet, integritet och tillgänglighet

Artikel 2 Olagligt intrång

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga orättmätigt intrång i hela eller en del av ett datorsystem, när det görs uppsåtligen. En part får uppställa krav på att brottet begås genom intrång i säkerhetsåtgärder med uppsåt att komma över datorbehandlingsbara uppgifter eller med annat brottsligt uppsåt

eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Artikel 3 Olaglig avlyssning

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen: att med tekniska hjälpmedel orättmätigt avlyssna icke allmänna överföringar av datorbehandlingsbara uppgifter till, från eller inom ett datorsystem, däribland elektromagnetiska emissioner från ett datorsystem med sådana datorbehandlingsbara uppgifter. En part får uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Artikel 4 Datastörning

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen:

Att orättmätigt skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

2. En part får förbehålla sig rätten att uppställa krav på att det handlande som anges i punkt 1 medför allvarlig skada.

Artikel 5 Systemstörning

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen: att orättmätigt allvarligt hindra ett datorsystems drift genom att mata in, överföra, skada,

radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

Artikel 6 Missbruk av apparatur

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt:

a) Att tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra

i) en apparat vari ingår ett datorprogram som är skapat eller anpassat främst för att begå något av de brott som straffbeläggs i enlighet med artiklarna 2-5,

ii) ett datorlösenord, en åtkomstkod eller liknande datorbehandlingsbara uppgifter som kan ge åtkomst till ett helt datorsystem eller en del därav

med uppsåt att den eller det skall användas för att begå något av de brott som straffbeläggs i enlighet med artiklarna 2-5.

b) Att inneha ett föremål som avses i a i eller a ii ovan med uppsåt att det skall användas för att begå något av de brott som straffbeläggs i enlighet med artiklarna 2-5. En part får i lag uppställa krav på att flera sådana föremål skall innehas för att straffansvar skall gälla.

2. Denna artikel skall inte tolkas som att den ålägger straffansvar i de fall där tillverkning, försäljning, anskaffning för användning, import, spridning eller annat tillgängliggörande eller innehav som avses i punkt 1 i denna artikel inte har till syfte att något av de brott som straffbeläggs i enlighet med artiklarna 2-5 i denna konvention skall begås, såsom exempelvis för att i behörig ordning testa eller skydda ett datorsystem.

3. Varje part får förbehålla sig rätten att inte tillämpa punkt 1 i denna artikel, om förbehållet inte avser försäljning, spridning eller annat tillgängliggörande av föremål som avses i punkt 1 a ii i denna artikel.

Avdelning 2 Datorrelaterade brott

Artikel 7 Datorrelaterad förfalskning

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt:

Att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter så att icke autentiska uppgifter uppstår med uppsåt att dessa skall beaktas eller ligga till grund för handlande i rättsliga hänseenden som om de vore autentiska, oavsett om uppgifterna är direkt läsbara och begripliga. En part får uppställa krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar skall gälla.

Artikel 8 Datorrelaterat bedrägeri

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt: att förorsaka en annan person förlust av egendom genom att

a) mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter,

b) störa ett datorsystems drift,

med bedrägligt eller annat brottsligt uppsåt och orättmätigt skaffa sig själv eller en annan person en ekonomisk förmån.

Avdelning 3 Innehållsrelaterade brott

Artikel 9 Brott som hänför sig till barnpornografi

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt:

a) Att framställa barnpornografi i syfte att sprida den med hjälp av datorsystem.

b) Att bjuda ut eller tillgängliggöra barnpornografi med hjälp av datorsystem.

c) Att sprida eller överföra barnpornografi med hjälp av datorsystem.

d) Att anskaffa barnpornografi åt sig själv eller någon annan med hjälp av datorsystem.

e) Att inneha barnpornografi i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter.

2. För de syften som avses i punkt 1 ovan skall termen *barnpornografi* innefatta pornografiskt material som visuellt avbildar

a) en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd,

b) en person som ser ut att vara en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd, och

c) realistiska bilder som föreställer en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd.

3. För de syften som avses i punkt 2 ovan skall termen *minderårig* innefatta alla personer under 18 års ålder. En part får dock kräva en lägre åldersgräns, som inte skall vara lägre än 16 år.

4. Varje part får förbehålla sig rätten att, helt eller delvis, inte tillämpa punkt 1 d - e och punkt 2 b - c i denna artikel.

Avdelning 4 Brott som hänför sig till intrång i upphovsrätt och närstående rättigheter

Artikel 10 Brott som hänför sig till intrång i upphovsrätt och närstående rättigheter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga intrång i upphovsrätt, som detta begrepp definieras i den partens lagstiftning, enligt de skyldigheter som parten har iklätt sig enligt Parisbeslutet av den 24 juli 1971 om revidering av Bernkonventionen för skydd av litterära och konstnärliga verk, avtalet om handelsrelaterade aspekter av immaterialrätter och WIPO-fördraget om upphovsrätt, med undantag för ideella rättigheter som erkänns i dessa konventioner, när sådana gärningar begås uppsåtligen, i kommersiell skala och med hjälp av ett datorsystem.

2. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga intrång i närstående rättigheter, som dessa definieras i den partens lagstiftning, enligt de skyldigheter den har iklätt sig enligt konventionen om skydd för utövande konstnärer, framställare av fonogram och radioföretag (Romkonventionen), avtalet om handelsrelaterade aspekter av immaterialrätter, WIPO-fördraget om framföranden och fonogram, med undantag för ideella rät-

tigheter som erkänns i dessa konventioner, när sådana gärningar begås uppsåtligen, i kommersiell skala och med hjälp av ett datorsystem.

3. En part får förbehålla sig rätten att inte införa straffansvar enligt punkterna 1 och 2 i denna artikel i begränsad omfattning, under förutsättning att andra effektiva rättsliga åtgärder kan komma i fråga och att förbehållet inte innebär ett avsteg från partens internationella skyldigheter enligt de internationella instrument som nämns i punkterna 1 och 2 i denna artikel.

Avdelning 5 Andra former av ansvar och påföljder

Artikel 11 Försök och medhjälp

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga uppsåtlig medhjälp till något av de brott som straffbeläggs i enlighet med artiklarna 2-10 i denna konvention med uppsåt att begå sådant brott.

2. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga uppsåtligt försök till något av de brott som straffbeläggs i enlighet med artiklarna 3-5, 7, 8 samt 9.1 a och 9.1 c i denna konvention.

3. Varje part får förbehålla sig rätten att, helt eller delvis, inte tillämpa punkt 2 i denna artikel.

Artikel 12 Juridiska personers ansvar

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att juridiska personer kan ställas till ansvar för gärningar som straffbeläggs i enlighet med denna kon-

vention, om de har begåtts till deras förmån av en fysisk person som handlat individuellt eller som en del av ett organ tillhörande den juridiska personen och som har en ledande ställning inom denna grundad på

a) en fullmakt att företräda den juridiska personen,

b) ett bemyndigande att fatta beslut på den juridiska personens vägnar, eller

c) ett bemyndigande att utöva kontroll inom den juridiska personen.

2. Utöver de fall som avses i punkt 1 i denna artikel skall varje part vidta nödvändiga åtgärder för att tillse att en juridisk person kan ställas till ansvar när bristande övervakning eller kontroll som skall utföras av en sådan fysisk person som avses i punkt 1 i denna artikel gjort det möjligt för en fysisk person, som handlar på den juridiska personens vägnar, att begå brott som straffbeläggs i enlighet med denna konvention till förmån för den juridiska personen.

3. Beroende på principerna i partens rättsordning, får den juridiska personens ansvar vara av straffrättslig, civilrättslig eller administrativ natur.

4. Sådant ansvar skall inte inverka på straffansvaret för de fysiska personer som har gjort sig skyldiga till gjort sig skyldiga till brottet.

Artikel 13 Påföljder och åtgärder

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att de brott som straffbeläggs i enlighet med artiklarna 2-11 är straffbara med effektiva, proportionella och avskräckande påföljder, innefattande frihetsberövande.

2. Varje part skall tillse att juridiska personer som fälls till ansvar i enlighet med artikel 12 underkastas effektiva, proportionella och avskräckande straffrättsliga eller icke straffrättsliga påföljder eller åtgärder, innefattande ekonomiska påföljder.

Avsnitt 2 Processrätt

Avdelning 1 Gemensamma bestämmelser

Artikel 14 De processrättsliga bestämmelsernas räckvidd

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att fastställa de befogenheter och förfaranden som föreskrivs i denna avdelning för särskilt angivna brottsutredningar eller rättsliga förfaranden.

2. Med undantag för vad som särskilt föreskrivs i artikel 21 skall varje part tillämpa de befogenheter och förfaranden som avses i punkt 1 i denna artikel på

a) brott som straffbeläggs i enlighet med artiklarna 2-11 i denna konvention,

b) andra brott som begåtts med hjälp av ett datorsystem och

c) insamling av bevis i elektronisk form om ett brott.

3. a) Varje part får förbehålla sig rätten att endast tillämpa de åtgärder som avses i artikel 20 på brott eller brottstyper som anges i förbehållet, under förutsättning att omfattningen av dessa brott eller brottstyper inte är mer begränsad än det urval av brott på vilka parten tillämpar de åtgärder som avses i artikel 21. Varje part skall överväga att begränsa ett sådant förbehåll för att möjliggöra bredast möjliga tillämpning av den åtgärd som avses i artikel 20.

b) När en part till följd av begränsningar i sin vid tiden för antagandet av denna konvention gällande lagstiftning inte kan tillämpa de åtgärder som avses i artiklarna 20 och 21 på meddelanden som överförs inom en tjänsteleverantörs datorsystem, som

i) drivs för en sluten användargrupp, och

ii) inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt,

får den parten förbehålla sig rätten att inte tillämpa dessa åtgärder på sådana meddelanden. Varje part skall överväga att begränsa ett sådant förbehåll för att möjliggöra bredast möjliga tillämpning av de åtgärder som avses i artiklarna 20 och 21.

Artikel 15 Villkor och garantier

1. Varje part skall tillse att det för införandet, genomförandet och tillämpningen av de befogenheter och förfaranden som avses i denna avdelning gäller de villkor och garantier som föreskrivs i dess nationella lagstiftning, vilka skall ge ett tillfredsställande skydd för mänskliga rättigheter och friheter, däribland de rättigheter som följer av de åtaganden parten har gjort genom 1950 års Europarådskonvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna, 1966 års FN-konvention om medborgerliga och politiska rättigheter samt andra tillämpliga internationella fördrag om mänskliga rättigheter, och i vilka proportionalitetsprincipen skall vara införlivad.

2. Sådana villkor och garantier skall, när så är lämpligt med tanke på arten av det förfarande eller den befogenhet det gäller, bl.a. innefatta rättslig eller annan oberoende tillsyn, de skäl som motiverar tillämpning samt begränsning av omfattningen och varaktigheten av befogenheten eller förfarandet.

3. I den utsträckning det är förenligt med allmänintresset, särskilt med sund rättskipning, skall varje part pröva vilken inverkan de befogenheter och förfaranden som avses i denna avdelning har på tredje mans rättigheter, skyldigheter och rättmätiga intressen.

Avdelning 2 Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

Artikel 16 Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att dess behöriga myndigheter genom föreläggande eller på liknande sätt skall kunna åstadkomma skyndsamt säkrande av särskilt angivna datorbehandlingsbara uppgifter, innefattande trafikuppgifter, som har lagrats med hjälp av ett datorsystem, särskilt i de fall där det finns anledning att förmoda att de datorbehandlingsbara uppgifterna löper särskild risk att gå förlorade eller förändras.

2. När en part verkställer punkt 1 i denna artikel genom ett föreläggande till en person om att säkra särskilt angivna lagrade datorbehandlingsbara uppgifter i denna persons besittning eller under denna persons kontroll, skall parten vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga personen att säkra och bevara de datorbehandlingsbara uppgifterna orubbade så länge som behövs, dock högst 90 dagar, för att göra det möjligt för de behöriga myndigheterna att begära att uppgifterna röjs. En part får föreskriva att ett sådant föreläggande sedan får förnyas.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga den som har de datorbehandlingsbara uppgifterna i sin vård eller en sådan annan person som skall

bevara dem att hemlighålla att sådana åtgärder vidtagits under så lång tid som föreskrivs i dess nationella lagstiftning.

4. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Artikel 17 Skyndsamt säkrande och partiellt röjande av trafikuppgifter

1. Varje part skall i fråga om trafikuppgifter som skall säkras enligt artikel 16 vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att

a) tillse att ett sådant skyndsamt säkrande av trafikuppgifter kan ske, oavsett om en eller flera tjänsteleverantörer har deltagit i överföringen av meddelandet, och

b) tillse att en tillräcklig mängd trafikuppgifter skyndsamt röjs för partens behöriga myndighet, eller för en person utsedd av denna myndighet, för att parten skall kunna identifiera tjänsteleverantörerna och den väg på vilken meddelandet överfördes.

2. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Avdelning 3 Skyldighet att lämna uppgifter

Artikel 18 Skyldighet att lämna uppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att förelägga

a) en person inom dess territorium att lämna ut särskilt angivna datorbehandlingsbara uppgifter som vederbörande har i sin be-

sittning eller under sin kontroll, och som lagras i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter, och

b) en tjänsteleverantör som erbjuder sina tjänster inom partens territorium att lämna ut abonnentuppgifter som hänför sig till sådana tjänster och som tjänsteleverantören har i sin besittning eller under sin kontroll.

2. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

3. För de syften som avses i denna artikel betyder termen *abonnentuppgifter* varje information i form av datorbehandlingsbara uppgifter eller uppgifter i annan form som innehas av en tjänsteleverantör och som hänför sig till andra uppgifter om dennes abonnenter än trafikuppgifter eller innehållsuppgifter och genom vilka kan fastställas

a) den typ av kommunikationstjänst som använts, de tekniska åtgärder som vidtagits för dem och tidsperioden för tjänsten,

b) abonnentens identitet, postadress eller geografiska adress, telefonnummer och annat accessnummer, information om fakturering och betalning, som är tillgänglig genom tjänsteavtalet eller tjänstearrangemanget,

c) övriga upplysningar om var kommunikationsutrustningen är belägen som är tillgängliga genom tjänsteavtalet eller tjänstearrangemanget.

Avdelning 4 Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter

Artikel 19 Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att genom husrannsakan eller på liknande sätt inom territoriet bereda sig åtkomst till

a) ett datorsystem eller en del därav och de datorbehandlingsbara uppgifter som lagras däri, och

b) ett medium för lagring av datorbehandlingsbara uppgifter i vilket uppgifter kan vara lagrade.

2. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att dess myndigheter, när de genom husrannsakan eller på liknande sätt bereder sig åtkomst till ett visst datorsystem eller en del därav enligt punkt 1 a och har anledning att tro att de eftersökta uppgifterna är lagrade i ett annat datorsystem eller en del av ett annat datorsystem inom dess territorium och sådana uppgifter är lagligen åtkomliga eller tillgängliga för det första systemet, skyndsamt skall kunna utvidga husrannsakan eller det liknande sättet till att bereda sig åtkomst till detta andra system.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att beslagta eller på liknande sätt säkra datorbehandlingsbara uppgifter som åtkommits enligt punkterna 1 och 2 i denna artikel. Dessa åtgärder skall innefatta behörighet att

a) beslagta eller på liknande sätt säkra ett datorsystem eller en del därav eller ett medium för lagring av datorbehandlingsbara uppgifter,

b) framställa och behålla en kopia av dessa datorbehandlingsbara uppgifter,

c) bevara de lagrade datorbehandlingsbara uppgifternas integritet,

d) göra de datorbehandlingsbara uppgifterna oåtkomliga eller avlägsna dem från det datorsystem till vilket åtkomst har beretts.

4. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att förelägga en person som har kunskap om ett datorsystems funktion eller om de åtgärder som tillämpas för att skydda de datorbehandlingsbara uppgifter som finns däri att, i den mån det är skäligt, lämna den information som är nödvändig för att möjliggöra de åtgärder som avses i punkterna 1 och 2 i denna artikel.

5. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Avdelning 5 Insamling i realtid av datorbehandlingsbara uppgifter

Artikel 20 Insamling i realtid av trafikuppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att

a) med tekniska hjälpmedel inom partens territorium insamla eller ta upp, och

b) ålägga en tjänsteleverantör, att inom dennes existerande tekniska förmåga

i) att med tekniska hjälpmedel inom partens territorium insamla eller ta upp, eller

ii) att samarbeta med och biträda de behöriga myndigheterna med insamling eller upptagning

av trafikuppgifter i realtid som hör till särskilt angivna meddelanden, som inom partens territorium överförs med hjälp av ett datorsystem.

2. Om en part, beroende på gällande principer i sin nationella rättsordning, inte kan vidta de åtgärder som avses i punkt 1 a i denna artikel, får den i stället vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att med tekniska hjälpmedel inom sitt territorium säkerställa insamling eller upptagning i realtid av trafikuppgifter som hänför sig till särskilt angivna meddelanden som överförs inom partens territorium.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga en tjänsteleverantör att hemlighålla det förhållandet att befogenhet som avses i denna artikel utövas och all information som har samband med denna.

4. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Artikel 21 Avlyssning av innehållsuppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att, med avseende på vissa allvarliga brott som bestäms i partens nationella lagstiftning, bemyndiga sina behöriga myndigheter att

a) med tekniska hjälpmedel inom partens territorium insamla eller ta upp, och

b) ålägga en tjänsteleverantör, att inom dennes existerande tekniska förmåga

i) att med tekniska hjälpmedel inom partens territorium insamla eller ta upp, eller

ii) att samarbeta med och biträda de behöriga myndigheterna med insamling eller upptagning

i realtid av innehållsuppgifter i särskilt angivna meddelanden inom partens territorium som överförs med hjälp av ett datorsystem.

2. Om en part, beroende på gällande principer i sin nationella rättsordning, inte kan vidta de åtgärder som avses i punkt 1 a ovan, får den i stället vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att med tekniska hjälpmedel inom dess territorium säkerställa insamling eller upptagning i realtid av innehållsuppgifter i särskilt angivna meddelanden, som överförs inom dess territorium.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga en tjänsteleverantör att hemlighålla det förhållandet att befogenhet som avses i denna artikel utövas och all information som har samband med denna.

4. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Avsnitt 3 Domsrätt

Artikel 22 Domsrätt

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att utöva domsrätt över brott som straffbe-

läggs i enlighet med artiklarna 2-11 i denna konvention, när brottet har begåtts

a) inom dess territorium, eller

b) ombord på ett fartyg som för dess flagg, eller

c) ombord på ett luftfartyg som är registrerat enligt dess lagar, eller

d) av en av dess medborgare, om brottet är straffbart enligt strafflagstiftningen där det begicks eller om brottet inte faller under någon stats territoriella behörighet.

2. Varje part får förbehålla sig rätten att inte alls tillämpa eller att bara i vissa fall och under särskilda förhållanden tillämpa de regler om domsrätt som anges i punkt 1 b - d i denna artikel eller en del av dessa regler.

3. Varje part skall vidta nödvändiga åtgärder för utöva domsrätt över de brott som avses i artikel 24.1 i denna konvention i de fall då en påstådd gärningsman befinner sig inom dess territorium och parten inte på begäran utlämnar honom eller henne till en annan part endast på grund av hans eller hennes nationalitet.

4. Denna konvention utesluter inte straffrättslig domsrätt som utövas av en part i enlighet med dess nationella lagstiftning.

5. I de fall där mer än en part gör gällande domsrätt över ett påstått brott som straffbeläggs enligt denna konvention, skall de berörda parterna, om så om det är lämpligt, samråda för att avgöra vilken domsrätt som är den lämpligaste för lagföring.

Kapitel 3 Internationellt samarbete

Avsnitt 1 Allmänna principer

Avdelning 1 Allmänna principer för internationellt samarbete

Artikel 23 Allmänna principer för internationellt samarbete

Parterna skall i största möjliga utsträckning samarbeta med varandra i enlighet med bestämmelserna i detta kapitel och genom tillämpning av relevanta internationella instrument om internationellt samarbete i straffrättsliga frågor, gällande överenskommelser som ingåtts på grundval av ensartad eller reciprok lagstiftning samt nationella lagar, för att utreda eller lagföra brott som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller för insamling av bevis i elektronisk form om brott.

Avdelning 2 Principer för utlämning

Artikel 24 Utlämning

1. a) Denna artikel tillämpas på utlämning mellan parter för brott som straffbeläggs i enlighet med artiklarna 2-11 i denna konvention, om brotten enligt lagstiftningen i båda de berörda parterna kan bestraffas med frihetsberövande och maximistraffet uppgår till lägst ett år, eller med strängare straff.

b) I de fall där ett annat lägsta straff skall tillämpas enligt en överenskommelse som ingåtts på grundval av ensartad eller reciprok lagstiftning eller ett utlämningsavtal, däribland europeiska utlämningskonventionen (ETS 24), som gäller mellan två eller flera parter, skall det lägsta straff som anges i en sådan överenskommelse eller ett sådant avtal gälla.

2. De brott som avses i punkt 1 i denna artikel skall anses tillhöra de utlämningsbara brotten i ett utlämningsavtal som gäller mel-

lan två eller flera parter. Parterna förbinder sig att ta med sådana brott bland de utlämningsbara brotten i utlämningsavtal som kommer att slutas mellan två eller flera av dem.

3. Om en part som för utlämning ställer som villkor att det finns ett utlämningsavtal mottar en framställning om utlämning från en annan part med vilken den inte har slutit ett sådant avtal, får den betrakta denna konvention som rättslig grund för utlämning för brott som avses i punkt 1 i denna artikel.

4. Parter som för utlämning inte ställer som villkor att utlämningsavtal skall föreligga skall erkänna de brott som avses i punkt 1 i denna artikel som utlämningsbara brott mellan dem.

5. För utlämning skall gälla de villkor som anges i den anmodade partens lagstiftning eller i gällande utlämningsavtal, däribland de skäl på grund av vilka den anmodade parten får vägra att bevilja utlämning.

6. Om utlämning för brott som avses i punkt 1 i denna artikel vägras endast på grund av den sökta personens nationalitet eller därför att den anmodade parten anser sig ha domsrätt över brottet, skall den anmodade parten efter framställning från den begärande parten hänskjuta ärendet till sina behöriga myndigheter för lagföring och rapportera slutresultatet till den begärande parten i vederbörlig ordning. Myndigheterna skall fatta beslut och genomföra utredningar och lagföring på samma sätt som för andra brott av jämförbar natur enligt den partens lagstiftning.

7. a) Varje part skall vid undertecknandet eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument meddela Europarådets generalsekreterare namn och adress på de myndigheter som är ansvariga för att göra eller ta emot framställningar om utlämning eller provisoriskt frihetsberövande i avsaknad av avtal.

b) Europarådets generalsekreterare skall upprätta och föra en aktuell förteckning över de myndigheter som utsetts på detta sätt av parterna. Varje part skall tillse att uppgifterna i förteckningen alltid är riktiga.

Avdelning 3 Allmänna principer för ömsesidig rättslig hjälp

Artikel 25 Allmänna principer för ömsesidig rättslig hjälp

1. Parterna skall i största möjliga utsträckning lämna varandra ömsesidig rättslig hjälp för att utreda och lagföra brott som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller för insamling av bevis i elektronisk form om brott.

2. Varje part skall också vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att uppfylla åtagandena i artiklarna 27-35.

3. Varje part får i brådskande fall göra framställningar om ömsesidig rättslig hjälp eller sända meddelanden relaterade därtill genom snabba kommunikationsmedel, däribland telefax eller elektronisk post, i den mån sådana medel tillgodoser tillräckliga säkerhetsnivåer och verifiering (däribland användning av kryptering vid behov) med efterföljande formell bekräftelse, i den mån så krävs av den anmodade parten. Den anmodade parten skall godta och besvara framställningar genom sådana snabba kommunikationsmedel.

4. Om inte annat uttryckligen föreskrivs i artiklarna i detta kapitel, skall för ömsesidig rättslig hjälp gälla de villkor som föreskrivs i den anmodade partens lagstiftning eller i tillämpliga avtal om ömsesidig rättslig hjälp, innefattande de skäl på grund av vilka den anmodade parten får avslå en framställning om samarbete. Den anmodade parten får inte vägra rättslig hjälp i fråga om brott som avses i artiklarna 2-11 endast av det skälet att framställningen gäller ett brott som den anser vara ett fiskalt brott.

5. I de fall där den anmodade parten, i enlighet med bestämmelserna i detta kapitel, har rätt att ställa dubbel straffbarhet som villkor för rättslig hjälp, skall det villkoret anses vara uppfyllt, oberoende av om dess lagstiftning placerar brottet inom samma kategori av brott eller rubricerar det med samma termer som den begärande parten, om det handlande som ligger bakom brottet för vilket hjälp har begärts utgör ett brott enligt dess lagstiftning.

Artikel 26 Upplysningar som lämnas på eget initiativ

1. En part får, inom gränserna för sin nationella lagstiftning och utan föregående framställning, överlämna information som erhållits inom ramen för dess egna utredningar till en annan part, när den anser att röjande av sådan information skulle kunna hjälpa den mottagande parten att inleda eller utföra utredningar om och lagföring av brott som är straffbara enligt denna konvention eller som skulle kunna föranleda en framställning av denna part om samarbete med stöd av detta kapitel.

2. Den part som lämnar sådan information får, innan uppgifterna lämnas, begära att de skall hemlighållas eller endast användas på vissa villkor. Om den mottagande parten inte kan tillmötesgå en sådan begäran, skall den meddela den förstnämnda parten, som då skall avgöra om informationen ändå kan överlämnas. Om den mottagande parten tar emot uppgifterna på sådana villkor, är den skyldig att följa dem.

Avdelning 4 Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal

Artikel 27 Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal

1. Bestämmelserna i punkterna 2-9 i denna artikel skall tillämpas om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp på grundval av ensartad eller reciprok lagstiftning mellan de berörda parterna. Bestämmelserna i denna artikel skall inte tillämpas när det finns ett sådant avtal, en sådan överenskommelse eller sådan lagstiftning, såvida inte de berörda parterna kommer överens om att tillämpa någon del eller hela återstoden av denna artikel i deras ställe.

2. a) Varje part skall utse en eller flera centralmyndigheter som skall ansvara för att sända och besvara framställningar om ömsesidig rättslig hjälp, verkställa sådana framställningar eller remittera dem till de myndigheter som är behöriga att verkställa dem.

b) Centralmyndigheterna skall kommunicera direkt med varandra.

c) Varje part skall vid undertecknandet eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument meddela Europarådets generalsekreterare namn och adress på de myndigheter som utses enligt denna punkt.

d) Europarådets generalsekreterare skall upprätta och föra en aktuell förteckning över de centralmyndigheter som utsetts på detta sätt av parterna. Varje part skall tillse att uppgifterna i förteckningen alltid är riktiga.

3. Framställningar om ömsesidig rättslig hjälp enligt denna artikel skall göras i enlighet med det förfarande som anges av den begärande parten, utom när det är oförenligt med den anmodade partens lagstiftning.

4. Den anmodade parten får, utöver de skäl för avslag som anges i artikel 25.4, avslå en framställning om hjälp, om

a) framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller

b) den anmodade parten anser att verkställande av framställningen sannolikt kan inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper eller andra viktiga intressen.

5. Den anmodade parten får uppskjuta verkställandet av en framställning om det skulle inkräkta på brottsutredningar eller lagföring som utförs av dess myndigheter.

6. Innan den anmodade parten avslår en framställning eller uppskjuter hjälp, skall den, där så är lämpligt efter att ha samrått med den begärande parten, pröva om framställningen kan bifallas till en del eller med förbehåll för sådana villkor som den anmodade parten anser vara nödvändiga.

7. Den anmodade parten skall ofördröjligen underrätta den begärande parten om utfallet av en framställning om hjälp. Skälen för avslag eller uppskjutande av hjälpen skall anges. Den anmodade parten skall också underrätta den begärande parten om de skäl som omöjliggör verkställandet av framställningen eller sannolikt kan försena det avsevärt.

8. Den begärande parten får anhålla om att den anmodade parten hemlighåller att en framställning har gjorts med stöd av detta kapitel liksom dess syfte, utom i den mån det är nödvändigt för dess verkställande att röja uppgiften. Om den anmodade parten inte kan tillmötesgå anhållan om hemlighållande, skall den ofördröjligen meddela den begärande parten, som då skall avgöra om framställningen ändå skall verkställas.

9. a) I brådskande fall får framställningar om ömsesidig rättslig hjälp eller därtill hörande meddelanden sändas direkt av den begärande partens rättsliga myndigheter till motsvarande myndighet i den anmodade parten. I dessa fall skall en kopia samtidigt sändas till den anmodade partens centralmyndighet via den begärande partens centralmyndighet.

b) En framställning eller ett meddelande enligt denna punkt får göras via Internationella kriminalpolisorganisationen (Interpol).

c) Om en framställning görs i enlighet med a i denna punkt och myndigheten inte är behörig att handlägga den, skall den remittera framställningen till behörig nationell myndighet och direkt meddela den begärande parten att så har skett.

d) En framställning eller ett meddelande enligt denna punkt som inte innefattar tvångsåtgärder får sändas direkt av den begärande partens behöriga myndigheter till den anmodade partens motsvarande myndigheter.

e) Varje part får vid undertecknandet av konventionen eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument meddela Europarådets generalsekreterare att framställningar enligt denna punkt av effektivitetsskäl skall ställas direkt till dess centralmyndighet.

Artikel 28 Sekretess och begränsningar i fråga om användning

1. Bestämmelserna i denna artikel skall tillämpas om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp på grundval av ensartad eller reciprok lagstiftning mellan de berörda parterna. Bestämmelserna i denna artikel skall inte tillämpas när det finns ett sådant avtal, en sådan överenskommelse eller sådan lagstiftning, såvida inte de berörda parterna kommer överens om att tillämpa någon del eller hela återstoden av denna artikel i deras ställe.

2. Den anmodade parten får göra lämnande av upplysningar eller material som svar på en framställning beroende av att de

a) hemlighålls i de fall framställningen om ömsesidig rättslig hjälp inte kan verkställas om så inte är fallet, eller

b) inte används för andra utredningar eller annan lagföring än som anges i framställningen.

3. Om den begärande parten inte kan uppfylla ett villkor som anges i punkt 2 i denna artikel, skall den genast meddela den andra parten, som då skall avgöra om upplysningarna ändå kan överlämnas. Om den begärande parten godtar villkoret, är den bunden av det.

4. En part som lämnar upplysningar eller material med ett förbehåll som avses i punkt 2 i denna artikel får begära att den andra parten förklarar hur den har använt upplysningarna eller materialet med avseende på detta villkor.

Avsnitt 2 Särskilda bestämmelser

Avdelning 1 Ömsesidig rättslig hjälp med provisoriska åtgärder

Artikel 29 Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

1. En part får anmoda en annan part att genom föreläggande eller på annat sätt åstadkomma skyndsamt säkrande av uppgifter som lagrats med hjälp av ett datorsystem inom den andra partens territorium och beträffande vilka den begärande parten avser att överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av uppgifterna.

2. En framställning om säkrande som görs med stöd av punkt 1 i denna artikel skall innehålla följande:

a) Namnet på den myndighet som begär säkrandet.

b) Den gärning som är föremål för brottsutredning eller lagföring och ett sammandrag omständigheterna.

c) De lagrade datorbehandlingsbara uppgifter som skall säkras och deras förhållande till brottet.

d) Alla tillgängliga upplysningar som identifierar den som vårdar de lagrade datorbehandlingsbara uppgifterna eller var datorsystemet finns.

e) Upplysning om varför säkrandet är nödvändigt.

f) Uppgift om att parten avser att överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av de lagrade datorbehandlingsbara uppgifterna.

3. När den anmodade parten mottar en framställning från en annan part, skall den vidta alla lämpliga åtgärder för att skyndsamt säkra de särskilt angivna uppgifterna i enlighet med sin nationella lagstiftning. I fråga om besvarande av en framställning skall dubbel straffbarhet inte uppställas som ett villkor för säkrandet.

4. En part som ställer dubbel straffbarhet som villkor för att besvara en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av lagrade uppgifter får, med avseende på andra brott än de som straffbeläggs i enlighet med artiklarna 2-11 i denna konvention, förbehålla sig rätten att avslå en framställning om säkrande enligt denna artikel, om den har skäl att tro att vill-

koret om dubbel straffbarhet inte kan uppfyllas när uppgifterna skall röjas.

5. Härutöver får en framställning om säkrande avslås endast om

a) framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller

b) den anmodade parten anser att verkställande av framställningen sannolikt kan inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper eller andra viktiga intressen.

6. Om den anmodade parten anser att säkrande inte kommer att trygga den framtida tillgängligheten till uppgifterna eller hota sekretessen för, eller på annat sätt störa den begärande partens brottsutredning, skall den ofördröjligen meddela den begärande parten, som då får avgöra om framställningen ändå skall verkställas.

7. Ett säkrande som verkställs som svar på en framställning som avses i punkt 1 i denna artikel skall gälla under en period om minst 60 dagar, för att den begärande parten skall kunna överlämna en framställning om husrannsakan eller liknande åtkomst, beslag eller liknande säkringsåtgärd eller röjande av uppgifterna. Sedan en sådan framställning mottagits, skall uppgifterna bevaras i avvaktan på ett beslut om framställningen.

Artikel 30 Skyndsamt röjande av säkrade trafikuppgifter

1. Om den anmodade parten, vid verkställandet av en framställning enligt artikel 29 om att säkra trafikuppgifter som rör ett särskilt angivet meddelande, upptäcker att en tjänsteleverantör i en annan stat har medverkat i överföring av meddelandet, skall den anmodade parten snabbt röja en tillräcklig mängd trafikuppgifter för den begärande parten för att identifiera tjänsteleve-

rantören och den väg på vilken meddelandet har överförts.

2. Röjande av trafikuppgifter enligt punkt 1 i denna artikel får underlåtas endast om

a) framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller

b) den anmodade parten anser att verkställande av framställningen sannolikt kan inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper eller andra viktiga intressen.

Avdelning 2 Ömsesidig rättslig hjälp med utredningsbefogenheter

Artikel 31 Ömsesidig rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter

1. En part får anmoda en annan part att genom husrannsakan eller på liknande sätt skaffa åtkomst till, genom beslag eller liknande åtgärd säkra eller att röja uppgifter som lagrats med hjälp av ett datorsystem inom den anmodade partens territorium, däribland uppgifter som har säkrats enligt artikel 29.

2. Den anmodade parten skall besvara framställningen med tillämpning av de internationella instrument, överenskommelser och lagar som avses i artikel 23 och i enlighet med andra tillämpliga bestämmelser i detta kapitel.

3 Framställningen skall besvaras skyndsamt när

a) det finns skäl att tro att uppgifterna i fråga löper särskild risk att gå förlorade eller förändras, eller

b) de instrument, överenskommelser och lagar som avses i punkt 2 i denna artikel på annat sätt föreskriver skyndsamt samarbete.

Artikel 32 Gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter med samtycke eller i de fall de är allmänt tillgängliga

En part får utan tillstånd av en annan part

a) bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga (öppna källor), oavsett var uppgifterna befinner sig geografiskt, eller

b) genom ett datorsystem inom sitt territorium bereda sig åtkomst till eller ta emot lagrade datorbehandlingsbara uppgifter som finns hos en annan part, om den förstnämnda parten erhåller lagligt och frivilligt samtycke av den person som har laglig rätt att röja uppgifterna för parten via det datorsystemet.

Artikel 33 Ömsesidig rättslig hjälp med insamling i realtid av trafikuppgifter

1. Parterna skall lämna varandra rättslig hjälp med insamling i realtid av trafikuppgifter som hör till särskilt angivna meddelanden som överförs med hjälp av ett datorsystem inom deras territorier. Med beaktande av bestämmelserna i punkt 2 i denna artikel, skall för denna hjälp gälla de villkor och förfaranden som anges i den nationella lagstiftningen.

2. Varje part skall lämna sådan hjälp åtminstone med avseende på brott för vilka insamling i realtid av trafikuppgifter skulle vara möjlig i ett motsvarande nationellt fall.

Artikel 34 Ömsesidig rättslig hjälp med avlyssning av innehållsuppgifter

Parterna skall, i den utsträckning det är tillåtet enligt gällande avtal och nationell lagstiftning, lämna varandra rättslig hjälp i fråga om insamling eller upptagning i realtid av innehållsuppgifter i särskilt angivna meddelanden som överförs med hjälp av ett datorsystem.

Avdelning 3 Nätverk (24/7)

Artikel 35 Nätverk (24/7)

1. Varje part skall utse en kontaktpunkt som skall vara tillgänglig 24 timmar om dygnet sju dagar i veckan för att säkerställa omedelbar hjälp vid utredning och lagföring av brott som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller för insamling av bevis i elektronisk form om brott. Denna hjälp skall innefatta underlättande av eller, om det är tillåtet i partens nationella lagar och praxis, direkt vidtagande av följande åtgärder:

a) tillhandahållande av teknisk rådgivning,

b) säkrande av uppgifter i enlighet med artiklarna 29 och 30, samt

c) insamling av bevis, tillhandahållande av rättslig information och lokalisering av misstänkta.

2. a) En parts kontaktpunkt skall kunna skyndsamt kommunicera med en annan parts kontaktpunkt.

b) Om en parts utsedda kontaktpunkt inte tillhör partens myndighet eller myndigheter som ansvarar för internationell rättslig hjälp eller utlämning, skall kontaktpunkten tillse att den är i

stånd att skyndsamt samverka med en eller flera sådana myndigheter.

3. Varje part skall tillse att utbildad och välutrustad personal är tillgänglig för att underlätta nätverkets verksamhet.

Kapitel IV Slutbestämmelser

Artikel 36 Undertecknande och ikraftträdande

1. Denna konvention skall stå öppen för undertecknande av Europarådets medlemsstater och de icke-medlemsstater som har deltagit i utarbetandet av konventionen.

2. Denna konvention skall ratificeras, godtas eller godkännas. Ratifikations-, godtagande- eller godkännandeinstrument skall deponeras hos Europarådets generalsekreterare.

3. Denna konvention träder i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då fem stater, varav minst tre medlemsstater i Europarådet, har uttryckt sitt samtycke till att vara bundna av konventionen i enlighet med bestämmelserna i punkterna 1 och 2 i denna artikel.

4. För en signatärstat som senare uttrycker sitt samtycke till att vara bunden av konventionen träder denna i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då den har uttryckt sitt samtycke till att vara bunden av konventionen i enlighet med bestämmelserna i punkterna 1 och 2 ovan.

Artikel 37 Anslutning till konventionen

1. Efter det att det att denna konvention har trätt i kraft kan Europarådets ministerkommitté efter samråd med konventions-

staterna och med deras enhälliga samtycke inbjuda en stat som inte är medlem av Europarådet och som inte har deltagit i konventionens utarbetande att ansluta sig till konventionen. Beslutet skall fattas med den majoritet som anges i artikel 20 d i Europarådets stadga och i enhällighet av ombuden för de konventionsstater som är berättigade att delta i ministerkommittén.

2. För en stat som ansluter sig till konventionen enligt punkt 1 ovan träder den i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter dagen för deponeringen av anslutningsinstrumentet hos Europarådets generalsekreterare.

Artikel 38 Territoriell tillämpning

1. En stat kan när den undertecknar konventionen eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument ange för vilket eller vilka territorier konventionen skall gälla.

2. En stat kan vid en senare tidpunkt genom en förklaring ställd till Europarådets generalsekreterare utsträcka tillämpningen av konventionen till ett annat territorium som anges i förklaringen. I förhållande till ett sådant territorium träder konventionen i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog förklaringen.

3. En förklaring som avgivits enligt de båda föregående punkterna kan, med avseende på ett territorium som har angivits i förklaringen, återtas genom ett meddelande ställt till Europarådets generalsekreterare. Återtagandet börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog meddelandet.

Artikel 39 Konventionens verkan

1. Konventionens syfte är att komplettera tillämpliga multilaterala eller bilaterala fördrag eller överenskommelser mellan parterna, däribland bestämmelserna i följande instrument:

- Europeiska utlämningskonventionen, öppnad för undertecknande i Paris den 13 december 1957 (ETS nr 24).

- Europeiska konventionen om inbördes rättshjälp i brottmål, öppnad för undertecknande i Strasbourg den 20 april 1959 (ETS nr 30).

- Tilläggsprotokollet till europeiska konventionen om inbördes rättshjälp i brottmål, öppnad för undertecknande i Strasbourg den 17 mars 1978 (ETS nr 99).

2. Om två eller flera parter redan har ingått en överenskommelse eller slutit ett fördrag om frågor som behandlas i denna konvention eller på annat sätt reglerat sina inbördes förhållanden beträffande sådana frågor, eller om de i framtiden gör det, skall de också ha rätt att tillämpa överenskommelsen eller fördraget i fråga eller att reglera sina förhållanden i enlighet därmed. Om parter emellertid reglerar sina förhållanden beträffande frågor som behandlas i konventionen på annat sätt än det som regleras häri, skall de göra detta på ett sätt som inte är oförenligt med konventionens syften och principer.

3. Ingenting i konventionen skall inverka på en parts övriga rättigheter, begränsningar, skyldigheter eller ansvar.

Artikel 40 Förklaringar

En stat får vid undertecknandet eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument, genom ett skriftligt meddelande ställt till Europarådets

generalsekreterare meddela att den begagnar sig av möjligheten att kräva ytterligare rekvisit enligt vad som anges i artiklarna 2, 3, 6.1 b, 7, 9.3 och 27.9 e.

Artikel 41 Tillämpning på federala stater

1. En federal stat får förbehålla sig rätten att åta sig skyldigheter enligt kapitel II i konventionen som är förenliga med grundprinciperna för förhållandet mellan dess centralregering och delstaterna och andra liknande territoriella enheter under förutsättning att den fortfarande kan samarbeta enligt kapitel III.

2. När en federal stat gör ett förbehåll enligt punkt 1, får den inte tillämpa villkoren i förbehållet för att undanta eller väsentligen minska sina skyldigheter att vidta åtgärder enligt kapitel II. Den skall generellt sörja för vidsträckta och effektiva rättsliga medel för att de åtgärder som avses i kapitel II skall kunna verkställas.

3. Med avseende på de bestämmelser i denna konvention vilkas tillämpning faller under behörigheten hos delstaterna eller andra territoriella enheter, vilka inte enligt federationens konstitutionella system är skyldiga att vidta lagstiftningsåtgärder, skall den federala regeringen underrätta delstaternas behöriga myndigheter om bestämmelserna med sin välvilliga rekommendation och uppmana dem att vidta lämpliga åtgärder för att ge bestämmelserna verkan.

Artikel 42 Förbehåll

En stat får när den undertecknar konventionen eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument genom ett skriftligt meddelande ställt till Europarådets generalsekreterare förklara att den begagnar sig av de möjligheter att göra förbehåll som anges i artiklarna 4.2, 6.3, 9.4,

10.3, 11.3, 14.3, 22.2, 29.4 och 41.1. Inget annat förbehåll får göras.

Artikel 43 Förbehållens status och återtagande

1. En part som har gjort ett förbehåll i enlighet med artikel 42 får helt eller delvis återta det genom ett meddelande till Europarådets generalsekreterare. Återtagandet börjar gälla den dag då generalsekreteraren mottog meddelandet. Om det i meddelandet anges att återtagandet av ett förbehåll skall börja gälla den dag som anges i meddelandet och denna dag infaller senare än den dag då generalsekreteraren mottog meddelandet, skall återtagandet gälla från den senare dagen.

2. En part som har gjort ett förbehåll som avses i artikel 42 skall återta detta, helt eller delvis, så snart som omständigheterna så medger.

3. Europarådets generalsekreterare får regelbundet fråga parter som har gjort ett eller flera förbehåll som avses i artikel 42 om möjligheterna att de återtar dem.

Artikel 44 Ändringar

1. Ändringar i denna konvention får föreslås av en part och skall av Europarådets generalsekreterare meddelas dess medlemsstater, de icke-medlemsstater som har deltagit i utarbetandet av konventionen samt stater som har anslutit sig till eller inbjudits att ansluta sig till konventionen i enlighet med bestämmelserna i artikel 37.

2. Ändringsförslag från en part skall tillställas Europarådets kommitté för brottsfrågor, som skall avge yttrande över den föreslagna ändringen till ministerkommittén.

3. Ministerkommittén skall överväga den föreslagna ändringen och kommitténs för brottsfrågor yttrande och får, efter samråd med de icke-medlemsstater som är parter i konventionen, anta ändringen.

4. Text till ändringar som har antagits av ministerkommittén i enlighet med punkt 3 i denna artikel skall meddelas parterna för godtagande.

5. En ändring som har antagits i enlighet med punkt 3 i denna artikel skall träda i kraft den trettionde dagen efter det att samtliga parter har meddelat generalsekreteraren sitt godtagande av ändringen.

Artikel 45 Tvistlösning

1. Europarådets kommitté för brottsfrågor skall hållas underrättad om tolkningen och tillämpningen av konventionen.

2. Om en tvist skulle uppstå mellan parter om tolkningen eller tillämpningen av denna konvention, skall de söka lösa tvisten genom förhandling eller andra fredliga medel efter deras eget val, inbegripet hänskjutande av tvisten till Europarådets kommitté för brottsfrågor, till en skiljedomstol vars avgöranden skall vara bindande för parterna, eller till Internationella domstolen, efter överenskommelse mellan de berörda parterna.

Artikel 46 Samråd mellan parterna

1. Parterna skall på lämpligt sätt regelbundet samråda i syfte att underlätta följande:

a) konventionens faktiska tillämpning och genomförande, innefattande identifiering av problem på området liksom verkan av förklaringar eller förbehåll som gjorts enligt konventionen,

b) informationsutbyte om rättslig, politisk eller teknisk utveckling av betydelse på området för IT-relaterade brott och bevisinsamling i elektronisk form,

c) prövning av möjliga tillägg till och ändringar av konventionen.

2. Europarådets kommitté för brottsfrågor skall fortlöpande informeras om utfallet av det samråd som avses i punkt 1ovan.

3. Europarådets kommitté för brottsfrågor skall på lämpligt sätt främja samråd som avses i punkt 1 i denna artikel och vidta nödvändiga åtgärder för att biträda parterna i deras strävanden att komplettera eller ändra konventionen. Senast tre år efter konventionens ikraftträdande skall Europarådets kommitté för brottsfrågor i samarbete med parterna genomföra en granskning av konventionens samtliga bestämmelser och, vid behov, rekommendera lämpliga ändringar.

4. Utom i de fall de bärs av Europarådet, skall kostnader som uppstår vid genomförandet av bestämmelserna i punkt 1 ovan bäras av parterna på ett sätt som de skall komma överens om.

5. Parterna skall biträdas av Europarådets sekretariat i att utföra sina funktioner enligt denna artikel.

Artikel 47 Uppsägning

1. En part får när som helst säga upp konventionen genom ett meddelande ställt till Europarådets generalsekreterare.

2. Uppsägningen börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog meddelandet.

Artikel 48 Meddelanden

Europarådets generalsekreterare skall meddela medlemsstaterna, de icke-medlemsstater som har deltagit i utarbetandet av konventionen och de stater som har anslutit sig till den eller inbjudits att ansluta sig till den om

a) undertecknanden,

b) deponering av ratifikations-, godtagande-, godkännande- och anslutningsinstrument,

c) dag för konventionens ikraftträdande enligt artiklarna 36 och 37,

d) förklaringar enligt artikel 40 eller förbehåll enligt artikel 42,

e) andra handlingar, underrättelser eller meddelanden som rör konventionen.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade, undertecknat denna konvention.

Upprättad i Budapest den 23 november 2001 på engelska och franska, vilka båda texter är lika giltiga, i ett enda exemplar, som skall deponeras i Europarådets arkiv. Europarådets generalsekreterare skall översända bestyrkta kopior till varje medlemsstat i Europarådet, de icke-medlemsstater som har deltagit i utarbetandet av konventionen och till de stater som har inbjudits att ansluta sig till den.

Bilaga 2 Tilläggsprotokoll till konventionen om IT-relaterad brottslighet om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem

Preliminär översättning

Strasbourg den 28 januari 2003

Medlemsstaterna i Europarådet och de övriga stater som är parter i konventionen om IT-relaterad brottslighet, som öppnades för undertecknande i Budapest den 23 november 2001, och har undertecknat detta protokoll,

som beaktar att Europarådets syfte är att skapa en fastare enhet mellan dess medlemmar,

som erinrar om att alla människor är födda fria och jämbördiga i fråga om värdighet och rättigheter,

som betonar behovet av att säkerställa ett fullständigt och verkningsfullt förverkligande av mänskliga rättigheter utan någon diskriminering eller åtskillnad, såsom de garanteras i europeiska och andra internationella instrument,

som är övertygade om att gärningar av rasistisk och främlingsfientlig natur utgör en kränkning av de mänskliga rättigheterna och ett hot mot ett lagbundet samhällsskick och demokratisk stabilitet,

som anser att den nationella och den internationella rätten behöver tillhandahålla adekvata rättsliga åtgärder mot propaganda av rasistisk och främlingsfientlig natur som bedrivs med hjälp av datorsystem,

som är medvetna om att propaganda för sådana gärningar ofta är straffbelagd i nationell lagstiftning,

som beaktar konventionen om IT-relaterad brottslighet, som föreskriver moderna och flexibla medel för internationellt samarbete, och som är övertygade om behovet av att harmonisera materiella lagbestämmelser som rör kampen mot rasistisk och främlingsfientlig propaganda,

som är medvetna om att datorsystem erbjuder medel utan tidigare motstycke för att underlätta yttrandefrihet och frihet att meddela sig i hela världen,

som erkänner att yttrandefriheten är en av de viktigaste grundvalarna i ett demokratiskt samhälle och en av de grundläggande förutsättningarna för samhällets framåtskridande och varje människas utveckling,

som emellertid är oroade över risken för felaktig användning eller missbruk av sådana datorsystem för att sprida rasistisk och främlingsfientlig propaganda,

som är medvetna om behovet av att säkerställa en lämplig avvägning mellan yttrandefrihet och effektiv bekämpning av gärningar av rasistisk och främlingsfientlig natur,

som erkänner att detta protokoll inte avser att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem,

som beaktar tillämpliga internationella rättsliga instrument på detta område, särskilt konventionen om skydd för de mänskliga

rättigheterna och de grundläggande friheterna och dess protokoll nr 12 om allmänt förbud mot diskriminering, de befintliga Europarådskonventionerna om samarbete på det straffrättsliga området, särskilt konventionen om IT-relaterad brottslighet, Förenta nationernas internationella konvention om avskaffande av alla former av rasdiskriminering av den 21 december 1965, Europeiska unionens gemensamma åtgärd av den 15 juli 1996, som antogs av rådet med stöd i artikel K.3 i fördraget om Europeiska unionen, om åtgärder mot rasism och främlingsfientlighet,

som välkomnar den senaste utvecklingen som ytterligare främjar internationell förståelse och internationellt samarbete i fråga om bekämpning av IT-relaterad brottslighet och rasism och främlingsfientlighet,

som även beaktar den handlingsplan som antogs av Europarådets stats- och regeringschefer vid deras andra toppmöte i Strasbourg den 10-11 oktober 1997 för att söka gemensamma svar på utvecklingen av nya informationsteknologier, som grundar sig på Europarådets normer och värderingar,

har kommit överens om följande.

Kapitel I Gemensamma bestämmelser

Artikel 1 Syfte

Syftet med detta protokoll är att med avseende på parterna i protokollet komplettera bestämmelserna i konventionen om IT-relaterad brottslighet som öppnades för undertecknande i Budapest den 23 november 2001 (nedan kallad *konventionen*) vad gäller kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem.

Artikel 2 Definition

1. I detta protokoll används denna definition:

rasistiskt och främlingsfientligt material: skrivet material, bild eller annan framställning av idéer eller teorier som förespråkar, främjar eller uppmuntrar till hat, diskriminering eller våld mot en enskild person eller en grupp av personer på grund av ras, hudfärg, härstamning, nationellt eller etniskt ursprung liksom även trosbekännelse, under förebärande av något av de förstnämnda karakteristika.

2. De termer och uttryck som används i protokollet skall tolkas på samma sätt som i konventionen.

Kapitel II Åtgärder som skall vidtas på nationell nivå

Artikel 3 Spridande av rasistiskt och främlingsfientligt material med hjälp av datorsystem

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärning när den begås uppsåtligen och orättmätigt:

Att sprida eller på annat sätt tillgängliggöra rasistiskt och främlingsfientligt material till allmänheten med hjälp av ett datorsystem.

2. En part får förbehålla sig rätten att inte införa straffansvar för handlande som anges i definitionen i punkt 1 i denna artikel när materialet enligt definitionen i artikel 2 punkt 1 förespråkar, främjar eller uppmuntrar diskriminering utan samband med hat eller våld, under förutsättning att andra effektiva åtgärder finns att tillgå.

3. Utan hinder av punkt 2 i denna artikel får en part förbehålla sig rätten att inte tillämpa punkt 1 vid de fall av diskriminering för vilka, beroende på etablerade principer om yttrandefrihet i partens rättssystem, parten inte kan föreskriva effektiva åtgärder som avses i punkt 2.

Artikel 4 Rasistiskt och främlingsfientligt motiverat hot

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärning när den begås uppsåtligen och orättmätigt:

Att med hjälp av ett datorsystem hota i) personer av det skälet att de tillhör en grupp som utmärks av ras, hudfärg, härstamning, nationellt eller etniskt ursprung liksom även trosbekännelse, under förebärande av något av de förstnämnda karakteristika, eller ii) en grupp personer som utmärks av något av dessa karakteristika med att begå brott som i partens nationella lagstiftning definieras som allvarliga.

Artikel 5 Rasistiskt och främlingsfientligt motiverad kränkning

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärning när den begås uppsåtligen och orättmätigt:

Att offentligen med hjälp av ett datorsystem kränka i) personer av det skälet att de tillhör en grupp som utmärks av ras, hudfärg, härstamning, nationellt eller etniskt ursprung liksom även trosbekännelse, under förebärande av något av de förstnämnda karakteristika, eller ii) en grupp personer som utmärks av dessa karakteristika.

2. En part får antingen

a) uppställa krav på att det brott som avses i punkt 1 i denna artikel resulterar i att personen eller gruppen av personer som avses i punkt 1 utsätts för hat, missaktning eller löje, eller

b) förbehålla sig rätten att helt eller delvis inte tillämpa punkt 1 ovan.

Artikel 6 Förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärning när den begås uppsåtligen och orättmätigt:

Att med hjälp av ett datorsystem sprida eller på annat sätt för allmänheten göra tillgängligt material som förnekar, grovt förringar, gillar eller rättfärdigar gärningar som utgör folkmord eller brott mot mänskligheten såsom dessa gärningar definieras i folkrätten och erkänns som sådana genom lagakraftvunna beslut av den internationella militärdomstol, som upprättades genom Londonavtalet av den 8 augusti 1945, eller av någon annan internationell domstol som upprättats genom relevanta internationella instrument och vars domsrätt erkänns av parten i fråga.

2. En part får antingen

a) uppställa krav på att förnekandet eller det grova förringande som avses i punkt 1 görs med uppsåt att uppmuntra till hat, diskriminering eller våld mot en enskild person eller en grupp av personer på grund av ras, hudfärg, härstamning, nationellt eller etniskt ursprung liksom även trosbekännelse, under förebärande av något av de förstnämnda karakteristika, eller

b) förbehålla sig rätten att helt eller delvis inte tillämpa punkt 1.

Artikel 7 Medhjälp

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga uppsåtlig och orättmätig medhjälp till något av de brott som kriminaliseras i enlighet med detta protokoll med uppsåt att ett sådant brott skall begås.

Kapitel III Förhållandet mellan konventionen och detta protokoll

Artikel 8 Förhållandet mellan konventionen och detta protokoll

1. Artiklarna 1, 12, 13, 22, 41, 44, 45 och 46 i konventionen skall i tillämpliga delar gälla detta protokoll.

2. Parterna skall utvidga tillämpningsområdet för de åtgärder som anges i artiklarna 14-21 och 23-35 i konventionen på artiklarna 2-7 i detta protokoll.

Kapitel IV Slutbestämmelser

Artikel 9 Uttryck för samtycke till att vara bunden

1. Detta protokoll skall stå öppet för undertecknande av de stater som har undertecknat konventionen. De kan uttrycka sitt samtycke till att vara bundna antingen genom

a) undertecknande utan förbehåll för ratifikation, godtagande eller godkännande, eller

b) undertecknande med förbehåll för ratifikation, godtagande eller godkännande, följt av ratifikation, godtagande eller godkännande.

2. En stat får inte underteckna detta protokoll utan förbehåll för ratifikation, godtagande eller godkännande eller deponera ett ratifikations-, godtagande- eller godkännandeinstrument, om den inte redan har deponerat eller samtidigt deponerar ett ratifikations-, godtagande- eller godkännandeinstrument avseende konventionen.

3. Ratifikations-, godtagande- och godkännandeinstrument skall deponeras hos Europarådets generalsekreterare.

Artikel 10 Ikraftträdande

1. Detta protokoll träder i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då fem stater har uttryckt sitt samtycke till att vara bundna av protokollet i enlighet med bestämmelserna i artikel 9.

2. För en stat som senare uttrycker sitt samtycke till att vara bunden av detta protokoll, träder det i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då staten undertecknade protokollet utan förbehåll för ratifikation, godtagande eller godkännande eller deponerade sitt ratifikations-, godtagande- eller godkännandeinstrument.

Artikel 11 Anslutning

1. Sedan detta protokoll har trätt i kraft får en stat som har anslutit sig till konventionen också ansluta sig till det.

2. Anslutning skall göras genom deponering hos Europarådets generalsekreterare av ett anslutningsinstrument, som börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter dagen för deponeringen.

Artikel 12 Förbehåll och förklaringar

1. Förbehåll och förklaringar som en part gör med avseende på en bestämmelse i konventionen skall också gälla detta protokoll, om inte parten förklarar något annat vid undertecknandet eller deponeringen av sitt ratifikations-, godtagande-, godkännande eller anslutningsinstrument.

2. En stat får när den undertecknar detta protokoll eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument genom ett skriftligt meddelande ställt till Europarådets generalsekreterare förklara att den begagnar sig av möjligheten att kräva ytterligare rekvisit enligt vad som anges i artiklarna 3, 5 och 6 i protokollet. Samtidigt får en part, med avseende på bestämmelserna i protokollet göra förbehåll som avses i artikel 22.2 och artikel 41.1 i konventionen, oavsett eventuella förbehåll som denna part har gjort enligt konventionen. Inget annat förbehåll får göras.

3. En stat får när den undertecknar detta protokoll eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument genom ett skriftligt meddelande ställt till Europarådets generalsekreterare förklara att den begagnar sig av möjligheten att kräva sådana ytterligare rekvisit som avses i artikel 5.2 a och artikel 6.2 a i detta protokoll.

Artikel 13 Förbehållens status och återtagande

1. En part som har gjort ett förbehåll i enlighet med artikel 12 skall helt eller delvis återta detta så snart som omständigheterna medger. Återtagandet börjar gälla den dag då generalsekreteraren mottar meddelandet. Om det i detsamma anges att återtagandet av ett förbehåll skall börja gälla en dag som anges där, och denna dag infaller efter den dag då generalsekreteraren mottog meddelandet, skall återtagandet börja gälla den senare dagen.

2. Europarådets generalsekreterare får regelbundet fråga de parter som har gjort ett eller flera förbehåll som avses i artikel 12 om utsikterna att de återtar förbehållen.

Artikel 14 Territoriell tillämpning

1. En part kan när den undertecknar detta protokoll eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument ange för vilket eller vilka territorier protokollet skall tillämpas.

2. En part kan vid en senare tidpunkt genom en förklaring ställd till Europarådets generalsekreterare utsträcka tillämpningen av protokollet till ett annat territorium som anges i förklaringen. I förhållande till ett sådant territorium träder protokollet i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog förklaringen.

3. En förklaring som avgivits enligt de båda föregående punkterna kan, med avseende på ett territorium som anges i förklaringen, återtas genom ett meddelande ställt till Europarådets generalsekreterare. Återtagandet börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog meddelandet.

Artikel 15 Uppsägning

1. En part får när som helst säga upp detta protokoll genom ett meddelande ställt till Europarådets generalsekreterare.

2. Uppsägningen börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog meddelandet.

Artikel 16 Meddelanden

Europarådets generalsekreterare skall meddela Europarådets medlemsstater, de icke-medlemsstater som har deltagit i utarbetandet av detta protokoll samt de stater som har anslutit sig till det eller inbjudits att ansluta sig till det om

a) undertecknanden,

b) deponering av ratifikations-, godtagande-, godkännande- och anslutningsinstrument,

c) dag för protokollets ikraftträdande enligt artiklarna 9-11,

d) andra handlingar, meddelanden eller underrättelser som rör protokollet.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade, undertecknat detta protokoll.

Upprättat i Strasbourg den 28 januari 2003 på engelska och franska, vilka båda texter är lika giltiga, i ett enda exemplar, som skall deponeras i Europarådets arkiv. Europarådets generalsekreterare skall översända en bestyrkt kopia till varje medlemsstat i Europarådet, de icke-medlemsstater som har deltagit i utarbetandet av detta protokoll samt till de stater som har inbjudits att ansluta sig till det.