Europarådets konvention om it-relaterad brottslighet

Betänkande av
Utredningen om it-brottskonventionen

Stockholm 2013

STATENS OFFENTLIGA UTREDNINGAR
SOU 2013:39

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-598 191 91
Ordertel: 08-598 191 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss – hur och varför. Statsrådsberedningen (SB PM 2003:2, reviderad 2009-05-02)
– En liten broschyr som underlättar arbetet för den som ska svara på remiss.
Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Textbearbetning och layout har utförts av Regeringskansliet, FA/kommittéservice.

Omslag: Elanders Sverige AB.

Tryckt av Elanders Sverige AB.
Stockholm 2013

ISBN 978-91-38-23950-6
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 27 oktober 2011 att tillkalla en särskild utredare med uppdrag att analysera behovet av författningsändringar för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll och lämna förslag till de författningsändringar som behövs för att möjliggöra ett svenskt tillträde till instrumenten (dir. 2011:98).

Till särskild utredare förordnades överåklagaren Nils Rekke.

Som experter i utredningen förordnades från och med den 1 december 2011 kriminalkommissarien Anders Ahlqvist (Rikspolisstyrelsen), advokaten Per Furberg (Setterwalls Advokatbyrå), kammaråklagaren Chatrine Rudström (Åklagarmyndigheten), kanslirådet Susanne Södersten (Justitiedepartementet) och professorn Per Ole Träskman (Lunds universitet).

Som experter förordnades vidare från och med den 21 augusti 2012 rättssakkunnige Walo von Greyerz (Justitiedepartementet) och från och med den 13 september 2012 kammaråklagaren Cecilia Trossmark (Ekobrottsmyndigheten).

Som sekreterare i utredningen anställdes från och med den 1 december 2011 hovrättsassessorn Anna Graninger.

Den 11 oktober 2012 beslutade regeringen att även ge utredningen i uppdrag att analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF och överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att beakta allvaret i storskaliga angrepp mot informationssystem (dir. 2012:102).

Utredningen, som har antagit namnet Utredningen om it-brottskonventionen (Ju 2011:12), överlämnar härmed betänkandet *Europarådets konvention om it-relaterad brottslighet* (SOU 2013:39).

Experterna har i allt väsentligt ställt sig bakom utredningens överväganden och förslag. Betänkandet har därför formulerats i vi-form.

Uppdraget är härmed slutfört.

Stockholm i maj 2013

Nils Rekke

/Anna Graninger

Innehåll

Bilagor

Sammanfattning

Vårt uppdrag

Utredningen har haft i uppdrag att analysera behovet av och lämna förslag till de författningsändringar som krävs för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet och dess tilläggsprotokoll.

Därutöver har vi i tilläggsdirektiv fått i uppdrag att analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF.

I uppdraget har vidare ingått att överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem.

Behovet av lagändringar mot bakgrund av konventionen och tilläggsprotokollet

Europarådets konvention om it-relaterad brottslighet har tre huvudsyften. Det första är att åstadkomma en tillnärmning av ländernas nationella straffrätt beträffande vissa gärningar. Det andra är att säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser behoven av att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta till vara bevisning i elektronisk form. Det tredje är att lägga grunden för ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott.

Konventionen öppnades för undertecknande den 23 november 2001 och trädde i kraft den 1 juli 2004. Hittills har 51 stater under-

tecknat konventionen och 39 stater ratificerat den. Majoriteten av EU:s medlemsstater har ratificerat konventionen liksom de övriga nordiska länderna. Sverige undertecknade konventionen samma dag som den upprättades, men har ännu inte ratificerat den.

Under arbetet med konventionen 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.

Tilläggsprotokollet öppnades för undertecknande den 28 januari 2003 och trädde i kraft den 1 mars 2006. Hittills har 37 stater undertecknat tilläggsprotokollet och 20 stater ratificerat det. Sverige undertecknade tilläggsprotokollet samma dag som det upprättades, men har ännu inte ratificerat det.

Vår bedömning är att svensk rätt redan uppfyller såväl konventionens som tilläggsprotokollets krav på *straffrättsliga* bestämmelser, under förutsättning att dels förslagen i regeringens proposition 2012/13:74 *Förfalsknings- och sanningsbrotten* antas av riksdagen, dels Sverige utnyttjar den möjlighet som finns i tilläggsprotokollet att kräva vissa ytterligare rekvisit för straffansvar när det gäller förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten.

Vad avser konventionens *processrättsliga* bestämmelser, till vilka tilläggsprotokollet hänvisar, gör vi bedömningen att lagstiftningsåtgärder krävs för att svensk rätt ska leva upp till konventionens krav i artikel 16 och 17. Artiklarna gäller skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och skyndsamt säkrande och partiellt röjande av trafikuppgifter. Vi bedömer också att det finns skäl att överväga att införa en sådan möjlighet till föreläggande att lämna information inom ramen för en husrannsakan som avses i konventionens artikel 19.4, även om svensk rätt formellt sett redan kan anses uppfylla de krav som ställs. I övrigt anser vi att svensk rätt redan uppfyller de krav som ställs med hänsyn till att vissa möjligheter till förbehåll finns.

När det gäller konventionens bestämmelser om *internationellt samarbete*, till vilka tilläggsprotokollet på samma sätt som när det gäller de processrättsliga bestämmelserna hänvisar, anser vi att lagstiftningsåtgärder krävs för att svensk rätt ska leva upp till konventionens krav i artiklarna 29 och 30, vilka avser rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och skyndsamt röjande av vissa trafikuppgifter (motsvarigheterna till artiklarna 16

och 17 på området för rättslig hjälp). I övrigt bedömer vi att svensk rätt redan uppfyller de krav som ställs.

Genomförandet av konventionen och tilläggsprotokollet i svensk rätt

Artikel 16 i konventionen innebär att det ska vara möjligt att skyndsamt säkra särskilt angivna lagrade datorbehandlingsbara uppgifter. Ett säkrande innebär att uppgifterna ska bevaras på ett betryggande sätt. Med uppgifter avses vilken typ av uppgifter som helst, dvs. såväl trafik-, innehålls- som abonnentuppgifter. Den grundläggande tanken bakom artikeln är att säkrandet ska göras på ett mindre ingripande sätt än genom exempelvis husrannsakan och beslag. Säkrandet är vidare tänkt att kunna ske såväl hos fysiska som juridiska personer, inklusive tjänsteleverantörer. Det ska kunna tillämpas såväl på de brott som straffbeläggs i enlighet med konventionen och på andra brott som begåtts med hjälp av ett datorsystem som generellt på insamling av bevis i elektronisk form om ett brott.

För att uppfylla kraven i artikeln föreslår vi att det i rättegångsbalken införs en möjlighet att förelägga någon att under viss tid bevara elektroniska uppgifter. Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott ska således kunna föreläggas att bevara uppgiften. I föreläggandet ska anges under hur lång tid uppgiften ska bevaras. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga 90 dagar. Om det finns särskilda skäl ska tiden för bevarande få förlängas med högst 30 dagar. Om det är möjligt ska föreläggandet ges skriftligt. I annat fall ska den som föreläggandet riktas mot så snart som möjligt få ett skriftligt bevis om beslutet. Meddelande om åtgärden får inte obehörigen föras vidare. Föreläggandet ska innehålla en underrättelse om detta.

Enligt vårt förslag ska ett bevarandeföreläggande inte få riktas mot den som skäligen kan misstänkas för brottet eller mot närstående till den misstänkte. Beslut om bevarandeföreläggande ska få meddelas av undersökningsledaren eller åklagaren. Den som ålagts ett bevarandeföreläggande ska få begära rättens prövning av det. För rättens prövning ska i tillämpliga delar gälla vad som gäller för prövning av beslag.

Om ett bevarandeföreläggande riktas mot en sådan leverantör som är skyldig att lagra trafikuppgifter enligt lagen (2003:389)om

elektronisk kommunikation föreslår vi att samma regler som gäller i fråga om åtgärder för att skydda uppgifter som ska lagras, ska gälla även för uppgift som omfattas av föreläggandet. Vidare ska motsvarande regler om rätt till ersättning för kostnader och om anpassning för utlämnande av uppgifter som gäller för lagring av trafikuppgifter gälla för uppgifter som ska bevaras.

Den som inte följer ett bevarandeföreläggande kan enligt vår mening i vissa situationer hållas straffrättsligt ansvarig enligt bestämmelsen om brytande av myndighets bud i 17 kap. 13 § brottsbalken. Straffansvar enligt 9 kap. 6 § rättegångsbalken kan utkrävas för den som utan tillstånd bryter mot skyldigheten att hemlighålla att säkringsåtgärder vidtagits.

För att uppfylla kraven i konventionens artikel 29 föreslår vi att möjligheten att förelägga någon som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften, räknas upp som en av de åtgärder som omfattas av rättslig hjälp enligt lagen (2000:562) om internationell rättslig hjälp i brottmål.

Enligt artikel 17 ska ett sådant skyndsamt säkrande av trafikuppgifter som avses i artikel 16 kunna äga rum oavsett om en eller flera tjänsteleverantörer har varit inblandade vid överföringen av ett meddelande. I många fall är flera tjänsteleverantörer involverade då elektroniska uppgifter överförs. Det är därför inte säkert att det är tillräckligt att trafikuppgifter hos enbart en av tjänsteleverantörerna i överföringskedjan säkras. För att det ska vara möjligt att förelägga samtliga de tjänsteleverantörer som deltagit vid överföringen att bevara trafikuppgifter krävs först att dessa kan identifieras. För att säkrande ska kunna äga rum hos de tjänsteleverantörer som varit delaktiga vid överföringen föreskriver artikel 17 att det ska vara möjligt att skyndsamt få tillgång till de uppgifter som krävs för att tjänsteleverantörerna och den väg på vilken meddelandet överfördes ska kunna spåras. Även säkrandet enligt artikel 17 ska kunna tillämpas såväl på de brott som straffbeläggs i enlighet med konventionen och på andra brott som begåtts med hjälp av ett datorsystem som generellt på insamling av bevis i elektronisk form om ett brott.

För att uppfylla kraven i artikel 17 föreslår vi att det i lagen om elektronisk kommunikation införs en skyldighet för leverantörer att till den myndighet som beslutat om ett bevarandeföreläggande lämna ut uppgift om vilka övriga leverantörer som har deltagit vid överföringen av det meddelande som omfattas av föreläggandet. Vi bedömer att det inte krävs några ytterligare lagstiftningsåtgärder än

denna för att uppfylla kraven i konventionens artikel 30 på rättslig hjälp med skyndsamt röjande av vissa trafikuppgifter.

Enligt konventionens artikel 19.4 ska det finnas en möjlighet i nationell rätt för 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 i systemet, att i den mån det är skäligt lämna den information som är nödvändig för att möjliggöra husrannsakan i it-miljö. Vi bedömer att de svenska reglerna om vittnesförhör inför rätta visserligen formellt sett får anses uppfylla de krav som ställs upp i artikeln, men att det ändå finns skäl att i svensk rätt införa en specifik möjlighet till föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö. Enligt brottsutredande myndigheter finns nämligen ett praktiskt behov av att införa en sådan möjlighet till föreläggande.

Vi föreslår därför en ny bestämmelse i rättegångsbalken som innebär att den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där får föreläggas att lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Ett beslut om föreläggande får meddelas av undersökningsledaren eller åklagaren. Föreläggandet ska dokumenteras.

Om någon skäligen kan misstänkas för brottet får enligt vårt förslag föreläggande inte riktas mot den misstänkte. Föreläggande får inte heller riktas mot den som, om åtal väcks, inte skulle vara skyldig att vittna i målet eller om sådan uppgift som de brottsutredande myndigheterna vill få tillgång till. Vägrar den förelagde att lämna upplysningar får på undersökningsledarens eller åklagarens begäran vittnesförhör med honom eller henne äga rum inför rätten. Om förhöret ska i tillämpliga delar gälla vad som föreskrivs om bevisupptagning utom huvudförhandling. En misstänkt får beredas tillfälle att närvara vid förhöret om det kan ske utan men för utredningen.

I tilläggsprotokollets artikel 6.1 uppställs krav på kriminalisering av gärningar som innebär att någon uppsåtligen och orättmätigt med hjälp av ett datorsystem sprider eller på annat sätt för allmänheten tillgängliggör material som förnekar, grovt förringar, gillar eller rättfärdigar gärningar som enligt folkrätten eller vissa internationella domstolar utgör folkmord eller brott mot mänskligheten. Vi föreslår att Sverige utnyttjar den möjlighet som finns att förklara att krav uppställs på att förnekandet eller det grova förringandet 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, eftersom svensk rätt då, genom främst bestämmelserna om hets mot folkgrupp och uppvigling, uppfyller artikelns krav på vad som ska vara straffbelagt.

Artiklarna 20 och 21 i konventionen gäller insamling i realtid av trafikuppgifter respektive avlyssning av innehållsuppgifter. Vi föreslår att Sverige avger förbehåll av innehåll att åtgärderna i artikel 20 endast tillämpas på sådana brott avseende vilka hemlig övervakning av elektronisk kommunikation kan användas och att förbehåll avges av innehåll att åtgärderna i artiklarna 20 och 21 inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt.

Behovet av lagändringar mot bakgrund av direktivet

Inom EU antogs 2005 ett rambeslut om angrepp mot informationssystem. Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF syftar till att ytterligare närma medlemsstaternas strafflagstiftning till varandra på området för angrepp mot informationssystem och att ändra och utöka bestämmelserna i rambeslutet. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna. Förhandlingarna om direktivet är i allt väsentligt slutförda. Det återstår för EU:s institutioner att formellt anta den text som har godkänts av företrädare för rådet och Europaparlamentet. Efter att direktivet antas har medlemsstaterna två år på sig att genomföra det.

Tyngdpunkten i direktivet utgörs av materiellt straffrättsliga bestämmelser. Bestämmelserna överensstämmer till stor del med de som finns i Europarådets konvention om it-relaterad brottslighet. Till skillnad från konventionen ställer direktivet emellertid precisa krav på vilka påföljder som ska kunna dömas ut för vissa av brotten i direktivet.

Enligt artikel 9.3 och 9.4 ska brotten olaglig systemstörning och olaglig datastörning i vissa fall vara belagda med ett maximistraff på minst tre respektive fem års fängelse. Svensk rätt uppfyller genom främst dataintrångsbestämmelsen direktivets krav på vilka handlingar som ska vara straffbelagda som olaglig systemstörning och olaglig datastörning. Straffskalan för dataintrång är böter eller fängelse i högst två år. Vi bedömer därför att straffskalan för dataintrång måste

skärpas för att Sverige ska kunna genomföra direktivet. Av artikel 9.2 följer vidare att vissa straffbara befattningar med verktyg ska vara belagda med ett maximistraff på minst två års fängelse. Svensk rätt uppfyller i denna del kravet på straffbarhet genom främst bestämmelserna om förberedelse till brott, bl.a. förberedelse till dataintrång. För förberedelse till dataintrång är det inte möjligt att döma till två års fängelse. Det krävs alltså även av detta skäl en skärpning av straffskalan för dataintrång.

I övrigt anser vi att svensk rätt redan uppfyller de krav som ställs i direktivet.

En särskild straffskala för grovt dataintrång

Straffskalan för brytande av post- eller telehemlighet sträcker sig från böter till fängelse två år. Enligt vår mening är den nuvarande straffskalan alltjämt väl avvägd. Något skäl att skärpa straffet för brytande av post- eller telehemlighet anser vi alltså inte finnas.

Även straffskalan för dataintrång sträcker sig från böter till fängelse två år. Den nuvarande straffskalan för dataintrång ger emellertid enligt vår uppfattning inte tillräckligt utrymme för att kunna beakta allvaret i storskaliga angrepp mot informationssystem. Av olika skäl är det inte alltid möjligt att vid sådana angrepp mot informationssystem tillämpa andra straffbestämmelser med högre straffskalor, såsom bestämmelserna om sabotage, grov skadegörelse och terroristbrott. Enligt vår mening finns det alltså vid sidan av direktivet kriminalpolitiska skäl för att skärpa straffskalan för dataintrång.

Vi föreslår därför att det införs en särskild straffskala för grovt dataintrång. Straffskalan ska sträcka sig från fängelse sex månader till fängelse sex år. Vid bedömande av om ett dataintrång är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art.

Bestämmelsen om dataintrång ska inte längre vara subsidiär i förhållande till straffbestämmelserna om brytande av post- eller telehemlighet och om intrång i förvar. Försök och förberedelse till grovt dataintrång ska vara straffbart.

Summary

Our remit

The Inquiry was tasked with analysing the need and making proposals for the legislative amendments required for Sweden to be able to accede to the Council of Europe Convention on Cybercrime and its Additional Protocol.

In supplementary terms of reference, we were also tasked with analysing the need and making proposals for the legislative amendments needed to implement the draft (not yet formally adopted) Directive of the European Parliament and of the Council on attacks against information systems, repealing Council Framework Decision 2005/222/JHA.

The remit also included considering the need for tougher penalties for breaches of postal or telecommunication secrecy, or data security, in order to allow greater scope to take more nuanced account of the seriousness of large-scale attacks on information systems.

The need for legislative amendments in light of the Convention and Additional Protocol

The Council of Europe Convention on Cybercrime has three main aims. The first is to bring national penal law provisions concerning certain offences more closely into alignment. The second is to ensure that there are national procedural law provisions that meet the need to investigate and take legal action against the offences dealt with in the Convention and other offences committed using computers, and to be able to utilise evidence in electronic form. The third is to pave the way for rapid and effective international co-operation to combat cybercrime.

The Convention was opened for signature on 23 November 2001 and entered into force on 1 July 2004. So far, 51 states have signed the Convention and 39 states have ratified it. The majority of the EU Member States have ratified the Convention, along with the other Nordic countries. Sweden signed the Convention on the day it was drawn up, but has not yet ratified it.

Several issues emerged during work on the Convention that were not settled. These were taken up in an Additional Protocol to the Convention. The Additional Protocol concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

The Additional Protocol was opened for signature on 28 January 2003 and entered into force on 1 March 2006. So far, 37 states have signed the Additional Protocol and 20 states have ratified it. Sweden signed the Additional Protocol on the day it was drawn up, but has not yet ratified it.

In our assessment, Swedish law already fulfils the requirements of both the Convention and the Additional Protocol with regard to *penal law* provisions, as long as the proposals in Government bill 2012/13:74 *Falsification offences and offences against the truth* are adopted by the Riksdag, and Sweden uses the possibility to set certain additional criminal liability requirements with regard to denial, gross minimisation, approval or justification of genocide or crimes against humanity.

With regard to the *procedural law* provisions of the Convention, to which the Additional Protocol refers, we consider that legislative measures are needed in order for Swedish law to conform to the requirements in Articles 16 and 17 of the Convention. The articles concern expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data. We also consider that there are grounds to consider introducing the kind of possibility to order the disclosure of information as part of a search referred to in Article 19.4 of the Convention, even though, in formal terms, Swedish law can be considered to already fulfil the requirements set. In other respects we consider that Swedish law already fulfils the requirements set, given the possibilities for reservations.

With regard to the provisions of the Convention concerning *international cooperation*, to which the Additional Protocol refers in the same way as for the procedural law provisions, we consider that legislative measures are needed in order for Swedish law to

conform to the requirements in Articles 29 and 30 of the Convention concerning judicial assistance for the expedited preservation of stored computer data and expedited disclosure of preserved traffic data (which correspond to Articles 16 and 17 in the area of judicial assistance). In other respects we consider that Swedish law already fulfils the requirements set.

Implementation of the Convention and Additional Protocol in Swedish law

Article 16 of the Convention states that it should be possible to obtain the expeditious preservation of specified computer data. Preservation means that data is stored securely. The term 'data' refers to any kind of data, i.e. traffic data, content data or subscriber information. The basic idea behind the article is that the preservation of data should be achieved less intrusively than by search and seizure. Furthermore, the intention is that it should be possible to preserve data from both natural and legal persons, including service providers. It should be applicable both to offences that are punishable under the Convention and other offences committed using a computer system, and generally to the collection of electronic evidence concerning an offence.

In order to meet the requirements contained in the article, we propose that a possibility to order a person to preserve electronic data for a given period be introduced into the Swedish Code of Judicial Procedure. Anyone who has certain data stored in electronic form that can reasonably be assumed to be of significance to the investigation of an offence could thereby be ordered to preserve that data. The order should specify how long the data must be preserved. The time period may not be longer than necessary, and no longer than 90 days in any case. If there are special grounds to do so, it should be possible to extend the time period by a maximum of 30 days. If possible the order should be issued in writing. Otherwise the person who is the subject of the order should receive written evidence of the decision as soon as possible. Communications concerning the measure may not be forwarded without authorisation. The order should contain information to this effect.

According to our proposal, a preservation order may not be issued to anyone who might reasonably be suspected of the offence or anyone closely associated with the suspect. Decisions to issue a

preservation order should be communicated by the leader of the investigation or the prosecutor. A person to whom a preservation order is issued should be able to demand a judicial review of the order. Such judicial reviews should, where appropriate, be subject to the rules that apply to reviews of seizures.

If a preservation order is issued to a service provider that is liable to store traffic data under the Electronic Communications Act (2003:389), we propose that the same rules that apply for measures to protect data to be stored should also apply to data covered by the order. Furthermore, corresponding rules on the right to compensation for costs and on adaptation for disclosure of data that apply to traffic data storage should apply to data to be preserved.

In our view, in certain situations it should be possible to hold anyone who fails to comply with a preservation order criminally liable under the provisions on breaches of official orders contained in Chapter 17, Section 13 of the Penal Code. Under Chapter 9, Section 6 of the Swedish Code of Judicial Procedure criminal liability may be enforced against anyone who, without authorisation, breaches an obligation to conceal the fact that a preservation measure has been taken.

In order to meet the requirements contained in Article 29 of the Convention, we propose that the possibility to order anyone who has certain data stored in electronic form that can reasonably be assumed to be of significance to the investigation of an offence to preserve that data should count as one of the measures covered by judicial assistance under the Act on International Judicial Assistance in Criminal Matters (2000:562).

Under Article 17, the expeditious preservation of traffic data referred to in Article 16 should be possible regardless of whether one or more service providers were involved in the transmission of a communication. In many cases, several service providers are involved when electronic data is transmitted. It is therefore not necessarily sufficient to preserve traffic data from just one of the service providers in the chain of transmission. For it to be possible to order all service providers involved in the transmission to preserve traffic data, it must first be possible to identify them. For it to be possible to preserve data from those service providers that have been involved in the transmission, Article 17 states that it must be possible to gain expeditious access to the data required to trace the service providers and the path through which the communication was transmitted. Preservation under Article 17 should also be

applicable both to offences that are punishable under the Convention and other offences committed using a computer system, and generally to the collection of electronic evidence concerning an offence.

In order to meet the requirements contained in Article 17, we propose that an obligation be introduced into the Electronic Communications Act for service providers to submit information concerning the other providers involved in transmission of the communication that is the subject of the preservation order to the authority that has decided to issue the order. In our assessment, no other legislative measures are needed in order to meet the requirements contained in Article 30 of the Convention concerning judicial assistance for the expedited disclosure of certain traffic data.

Under Article 19.4 of the Convention, national legislation must empower the competent authorities to order any person who has knowledge about the functioning of a computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information to enable searches of the IT environment to be undertaken. In our view, although the Swedish rules on the examination of witnesses in court can certainly be considered to meet the requirements of the article in formal terms, there are still grounds to introduce a specific possibility to order the disclosure of information into Swedish law with the aim of facilitating searches in IT environments. This is because there is, according to the criminal investigation authorities, a practical need to introduce the possibility to issue this kind of order.

We therefore propose a new provision in the Swedish Code of Judicial Procedure stating that anyone who can be assumed to be familiar with the functions of a given computer system or other requirements for accessing it and examining the data in it may be ordered to provide the necessary instructions for a search to be conducted. A decision to issue an order may be communicated by the investigation leader or the prosecutor. The order must be documented.

Under our proposal, if anyone can reasonably be suspected of the offence, the order cannot be issued to the suspect. Nor may an order be issued to anyone who, if prosecution proceedings are initiated, would not be obliged to testify in the case or with regard to the data that the criminal investigation authorities wish to access. If the subject of the order refuses to disclose information, the investigation leader or prosecutor may demand that they be examined

before a court. This examination should be subject to the appropriate parts of the rules that apply to the taking of evidence outside of a main hearing. A suspect may be given the opportunity to attend the examination if this will not harm the investigation.

Article 6.1 of the Additional Protocol requires the criminalisation of acts whereby a person intentionally, and without right, uses a computer system to distribute or otherwise make available to the public material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined in international law or certain international courts. We propose that Sweden take the opportunity to declare a requirement that the offences of denial or gross minimisation are committed with intent to incite hatred, discrimination or violence against an individual or group on grounds of race, skin colour, origin, national or ethnic roots, or faith, because Swedish law would then meet the criminalisation requirements contained in the article, primarily through the provisions on agitation against a national or ethnic group and incitement to rebellion.

Articles 20 and 21 of the Convention concern the real-time collection of traffic data and the interception of content data respectively. We propose that Sweden enter a reservation of substance to the effect that the measures in Article 20 should only apply to offences for which secret surveillance of electronic communications can be used, and that a reservation of substance be entered to the effect that the measures in Articles 20 and 21 should not apply to communications transmitted solely through an electronic communications network that is relatively insignificant from a general communication standpoint.

Need for legislative amendments in light of the Directive

In 2005, a framework decision concerning attacks on information systems was adopted within the EU. The Directive of the European Parliament and of the Council on attacks against information systems, repealing Council Framework Decision 2005/222/JHA, aims to bring the Member States' criminal legislation into greater alignment in the area of attacks on information systems, and to amend and expand the provisions in the framework decision. A further aim is to improve cooperation between authorities and law enforcement bodies in the Member States. The negotiations on the Directive

have, in essence, been concluded. It remains for the EU institutions to formally adopt the text that has been approved by representatives in the Council and the European Parliament. Once the Directive is adopted the Member States have two years to implement it.

The central point of the Directive consists of material criminal law provisions. These provisions largely correspond to those found in the Council of Europe Convention on Cybercrime. Unlike the Convention, however, the Directive sets specific requirements for the penalties that can be imposed for certain offences outlined in the text.

Under Articles 9(3) and 9(4), the offences of illegal system interference and illegal data interference should, in some cases, respectively be punishable by a maximum penalty of at least three years' or five years' imprisonment. Primarily through the provisions on data security breaches, Swedish law meets the requirements contained in the Directive with regard to the actions that should be punishable as illegal system interference and illegal data interference. The scale of penalties for data security breaches is a fine or a maximum of two years' imprisonment. We therefore consider that the scale of penalties for data security breaches must be tougher in order for Sweden to be able to implement the Directive. Furthermore, Article 9(2) states that certain the criminal use of various tools should be punishable by a maximum penalty of two years' imprisonment. Swedish law meets the punishability requirement, primarily through the provisions on preparation to commit an offence, including preparation to commit a data security breach. However, preparation to commit a data security breach cannot be punished by two years' imprisonment. This is another reason why the scale of penalties for data security breaches needs to be tougher.

In other respects we consider that Swedish law fulfils the requirements set out in the Directive.

A special scale of penalties for gross breaches of data security

The scale of penalties for breaches of postal or telecommunication secrecy ranges from fines to two years' imprisonment. In our view, the current scale of penalties is still well-balanced. There is therefore no reason to introduce a tougher scale of penalties for breaches of postal or telecommunication secrecy.

The scale of penalties for breaches of data security also ranges from fines to two years' imprisonment. In our view, however, the current penalty scale for data security breaches does not allow sufficient scope to take account of the seriousness of large-scale attacks on information systems. For various reasons, in the case of such attacks on information systems it is not always possible to apply other penalty provisions involving higher penalty scales, such as those concerning sabotage, gross vandalism or terrorist offences. In our view therefore, even aside from the Directive there are criminal policy grounds to introduce a tougher scale of penalties for data security breaches.

We therefore propose the introduction of a special scale of penalties for gross breaches of data security. The scale should range from six months' to six years' imprisonment. When assessing whether a breach of data security is gross, special attention should be paid to whether the act caused, or could have caused, serious damage, targeted a large volume of data or was otherwise of a particularly dangerous nature.

The provision on breaches of data security should no longer be subsidiary to the penalty provisions concerning breaches of postal or telecommunication secrecy and intrusion into a safe depository. Attempts and preparations to commit gross breaches of data security should be punishable offences.

1 Författningsförslag

1.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att det i rättegångsbalken ska införas tre nya paragrafer, 27 kap. 16 och 16 a §§ samt 28 kap. 7 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	27 kap.
	16 §[1]
	Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott får föreläggas att bevara uppgiften.
	I föreläggandet ska anges under hur lång tid uppgiften ska bevaras. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga 90 dagar. Om det finns särskilda skäl får tiden för bevarande förlängas med högst 30 dagar.
	Föreläggande får inte riktas mot den som skäligen kan misstänkas för brottet eller någon honom eller henne sådan närstående person som avses i 36 kap. 3 §.

[1] Tidigare 16 § upphävd genom 1989:650.

16 a §

Föreläggande enligt 16 § beslutas av undersökningsledaren eller åklagaren. Om det är möjligt ska föreläggandet ges skriftligt. I annat fall ska den förelagde så snart som möjligt få ett skriftligt bevis om beslutet.

Meddelande om åtgärden får inte obehörigen föras vidare. Föreläggandet ska innehålla en underrättelse om detta.

Den som ålagts föreläggandet får begära rättens prövning av föreläggandet. För rättens prövning gäller i tillämpliga delar vad som sägs i 6 §.

28 kap.

7 a §

Undersökningsledaren eller åklagaren får förelägga den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där att lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Beslut om föreläggande ska dokumenteras.

Om någon skäligen kan misstänkas för brottet får föreläggande inte riktas mot den misstänkte. Föreläggande får inte heller riktas mot den som, om åtal väcks, inte skulle vara skyldig att vittna i målet om omständighet som avses i första stycket.

Vägrar den förelagde att lämna upplysningar får på undersök-

ningsledarens eller åklagarens begäran vittnesförhör med honom eller henne äga rum inför rätten. Om förhöret gäller i tillämpliga delar vad som föreskrivs om bevisupptagning utom huvudförhandling. En misstänkt får beredas tillfälle att närvara vid förhöret om det kan ske utan men för utredningen.

Denna lag träder i kraft den 1 januari 2015.

1.2 Förslag till lag om ändring i brottsbalken

Härigenom föreskrivs att 4 kap. 9 c och 10 §§ brottsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	9 c §[2]
Den som *i annat fall än som sägs i 8 och 9 §§* olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för *dataintrång* till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.	Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för *dataintrång* till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. *Om brottet är grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art.*
	10 §[3]
För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott	För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott

[2] Senaste lydelse 2007:213.
[3] Senaste lydelse 2004:406.

döms till ansvar enligt vad som sägs i 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt *eller* till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa.	döms till ansvar enligt vad som sägs i 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt, till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa, *eller till grovt dataintrång.*

Denna lag träder i kraft den 1 januari 2015.

1.3 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 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 4 kap. 24 c §, samt närmast före 4 kap. 24 c § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[4]	
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,	
	6. föreläggande enligt 27 kap. 16 § rättegångsbalken,
6. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	*7.* hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
7. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	*8.* tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
8. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	*9.* tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
9. hemlig kameraövervakning,	*10.* hemlig kameraövervakning,
10. hemlig rumsavlyssning,	*11.* hemlig rumsavlyssning,

[4] Senaste lydelse 2012:284.

11. överförande av frihetsberövade för förhör m.m., och	*12.* överförande av frihetsberövade för förhör m.m., och
12. rättsmedicinsk undersökning av en avliden person.	*13.* 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 §[5]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–*6*, *9*, *10* och *12* ska 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–*7*, *10*, *11* och *13* ska 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 *7, 8* och *11* lämnas enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *8*, *9* och *12* lämnas enligt de särskilda bestämmelserna i denna lag.

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

2 §[6]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *7* och *11* 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, *6*, *8–10* och *12* får endast lämnas	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *6*, *8* och *12* 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*, *9–11* och *13* får endast lämnas

[5] Senaste lydelse 2007:982.
[6] Senaste lydelse 2007:982.

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.	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.

4 §[7]

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 ska höras,

– namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a och 29 §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.	I 4 kap. 8, 11, 14, 24 a, *24 c,* 25, 25 b, 25 c, 26 a och 29 §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

Om ärendet är brådskande eller om verkställighet önskas inom viss tidsfrist, ska detta anges och motiveras.

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

4 kap.

Föreläggande enligt 27 kap. 16 § rättegångsbalken

24 c §

En ansökan om föreläggande enligt 27 kap. 16 § rättegångsbalken handläggs av åklagare.

[7] Senaste lydelse 2011:906.

Av ansökan ska framgå sådana uppgifter som behövs för att åtgärden ska kunna genomföras.

Åklagaren ska genast pröva om det finns förutsättningar för åtgärden. Om åtgärden beslutas ska denna gälla för en period om minst 60 dagar.

Denna lag träder i kraft den 1 januari 2015.

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

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

dels att 6 kap. 5, 16 c, 16 d, 21 och 22 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 6 kap. 16 g §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
5 §[8]	
Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a eller 16 c §.	Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a eller 16 c § *eller om uppgifterna begärts bevarade enligt 27 kap. 16 § rättegångsbalken*.
16 c §[9]	
Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2, 27 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kom-	Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 *eller 9*, 27 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kom-

[8] Senaste lydelse 2012:127.
[9] Senaste lydelse 2012:285.

munikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

munikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

16 d §[10]

Uppgifter som avses i 16 a § ska lagras i sex månader räknat från den dag kommunikationen avslutades. Vid utgången av denna tid ska den lagringsskyldige genast utplåna dem, om annat inte följer av andra stycket.

Om uppgifter som avses i första stycket begärts utlämnade före utgången av den föreskrivna lagringstiden men uppgifterna inte har hunnit lämnas ut, ska den lagringsskyldige lagra uppgifterna till dess så har skett och därefter genast utplåna de lagrade uppgifterna.

Om uppgifter som avses i första stycket begärts utlämnade *eller om uppgifter begärts bevarade enligt 27 kap. 16 § rättegångsbalken* före utgången av den föreskrivna lagringstiden men uppgifterna inte har hunnit lämnas ut *eller tiden för bevarande inte har löpt ut*, ska den lagringsskyldige lagra uppgifterna till dess så har skett och därefter genast utplåna de lagrade uppgifterna.

16 g §

Om någon som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § förelagts att bevara viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken gäller vad som sägs i 3 a § om åtgärder för att skydda uppgifter som ska lagras enligt 16 a § även för uppgift som ska bevaras enligt 27 kap. 16 § rättegångsbalken. Vidare gäller vad som sägs i 16 e § om rätt till ersättning för kostnader och i 16 f § om anpassning för utlämnande av uppgifter på motsvarande sätt även för

[10] Senaste lydelse 2012:127.

uppgift som ska bevaras enligt 27 kap. 16 § rättegångsbalken.

21 §[11]

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,

2. angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *och*

5. begäran om utlämnande av uppgift om abonnemang enligt 22 § första stycket 2.

4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,

5. begäran om utlämnande av uppgift om abonnemang enligt 22 § första stycket 2,

6. föreläggande att bevara uppgifter enligt 27 kap. 16 § rättegångsbalken, och

7. begäran om utlämnande av uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster enligt 22 § första stycket 9.

[11] Senaste lydelse 2012:285.

22 §[12]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska 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 (2010:1932), 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 ska ingripa mot brottet,

3. uppgift som avses i 20 § första stycket 1 och 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa,

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och 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 som avser 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 ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

7. 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 ska kunna

7. 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 ska kunna

[12] Senaste lydelse 2012:285.

fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, *och*	fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,
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.	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, *och*
	9. uppgift om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande enligt 27 kap. 16 § första stycket rättegångsbalken till den myndighet som meddelat föreläggandet.

Ersättning för att lämna ut andra uppgifter enligt första stycket 8 än lokaliseringsuppgifter ska vara skälig med hänsyn till kostnaderna för utlämnandet.

Denna lag träder i kraft den 1 januari 2015.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Utredningens ursprungliga direktiv

Utredningens ursprungliga direktiv beslutades av regeringen den 27 oktober 2011 (dir. 2011:98). Direktiven finns bifogade som *bilaga 1*.

Utredningens uppdrag enligt direktiven är att analysera behovet av författningsändringar för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet och dess tilläggsprotokoll och att lämna förslag till de författningsändringar som behövs för att möjliggöra ett svenskt tillträde till instrumenten.

Tilläggsdirektiven av den 11 oktober 2012

Regeringen beslutade den 11 oktober 2012 om tilläggsdirektiv till utredningen (dir. 2012:102). Tilläggsdirektiven finns bifogade som *bilaga 2*.

Enligt tilläggsdirektiven ska utredningen analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF. Utredningen ska vidare överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem.

2.2 Utredningens arbete

Utredningsarbetet påbörjades i december 2011. Utredningen har haft nio sammanträden, varav ett i form av ett tvådagars internatsammanträde.

Utredningen (huvudsakligen utredaren och sekreteraren) har samrått med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden och Post- och telestyrelsen.

Utredningen har följt beredningen inom Regeringskansliet med bl.a. betänkandena *Urkunden i tiden* (SOU 2007:92), *Förundersökning – objektivitet, beslag, dokumentation m.m.* (SOU 2011:45) och *Utlämning* (2011:71) samt med lagrådsremissen *De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation*, som under utredningstiden lett till lagstiftning. Vidare har utredningen följt relevant arbete inom EU, bl.a. förhandlingarna om förslaget till direktiv om angrepp mot informationssystem (KOM[2010] 517 slutlig), förslaget till direktiv om en europeisk utredningsorder (2010/C 165/02) och utvärderingen av Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG. Utredningen har även följt arbetet i riksdagen med de tidigare vilande lagförslagen i propositionen om genomförandet av sistnämnda direktiv (bet. 2010/11:JuU14, rskr. 2010/11:189) samt Yttrandefrihetskommitténs (dir 2007:76) och Utredningens om vissa hemliga tvångsmedel (Ju 2010:08) arbete.

Information om lagstiftning från andra nordiska länder har inhämtats dels genom sökningar i databaser, dels genom kontakter med företrädare för utländska myndigheter och universitet.

Från Brottsförebyggande rådet (Brå) har utredningen inhämtat vissa statistikuppgifter.

Den särskilde utredaren och sekreteraren har deltagit vid en konferens om it-brott arrangerad av Europäische Rechtsakademie (ERA), den 24–25 maj 2012 i Milano. Den särskilde utredaren och några av experterna har vidare deltagit i dels en konferens syftande till att ytterligare stärka samarbetet mellan USA och Sverige när det gäller it-relaterad brottslighet, arrangerad av det svenska och amerikanska justitiedepartementet samt svensk och amerikansk polis, den 11–12 oktober 2012 i Stockholm, dels en konferens om it-

relaterad ekonomisk brottslighet, arrangerad av Ekobrottsmyndigheten, den 25–26 oktober 2012 i Stockholm. Den särskilde utredaren har även sammanträffat med företrädare för den kommitté inom Europarådet som övervakar Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll (the Cybercrime Convention Committee [T-CY]).

2.3 Disposition av betänkandet

Betänkandet omfattar 12 kapitel. I kapitel 3 finns en kort bakgrund till konventionen, tilläggsprotokollet och direktivet. Därefter följer i kapitel 4 avsnitt om det huvudsakliga innehållet i de tre instrumenten. Dessa inledande kapitel är deskriptiva till sin karaktär.

Våra överväganden och förslag redovisas i kapitel 5–9. I kapitel 5 analyserar vi med utgångspunkt i konventionens artiklar de behov av lagändringar som konventionen föranleder. I kapitel 6 och 7 görs motsvarande analys i förhållande till tilläggsprotokollet (kapitel 6) och direktivet (kapitel 7). I kapitel 8 ger vi, mot bakgrund av de analyser vi gjort i kapitel 5 och 6, förslag till hur konventionen och tilläggsprotokollet ska genomföras i svensk rätt. I kapitel 9 överväger vi behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång och lämnar, delvis mot bakgrund av analysen i kapitel 7, förslag till en särskild straffskala för grovt dataintrång.

Kapitel 10 innehåller kostnads- och konsekvensanalys och kapitel 11 förslag i fråga om ikraftträdande. Kapitel 12, slutligen, innehåller utredningens författningsförslag med kommentarer. Författningsförslagen är som brukligt också, jämte sammanfattningen, redovisade inledningsvis i betänkandet.

3 Bakgrund

Tillkomsten av Europarådets konvention om it-relaterad brottslighet (ETS nr 185), Rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem och Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF, ska ses mot bakgrund av de genomgripande förändringar i samhället som datoriseringen och de globala datornätverken har fört med sig. Dagens samhälle präglas av att informationsteknik genomsyrar i stort sett alla sektorer. Det innebär samtidigt att samhället är sårbart för olika former av angrepp som riktar sig mot tekniken, såsom olovliga intrång i informationssystem samt störningar av sådana system och av uppgifter i systemen. En effektiv kamp mot it-relaterad brottslighet kräver ett utvidgat, snabbt och väl fungerande internationellt samarbete.

I november 1996 beslutade Europarådets styrkommitté 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.

Konventionen öppnades för undertecknande den 23 november 2001 och trädde i kraft den 1 juli 2004. Hittills (per den 20 maj 2013) har 51 stater undertecknat konventionen och 39 stater ratificerat den. Majoriteten av EU:s medlemsstater har ratificerat konventionen liksom de övriga nordiska länderna. Även stater som inte är medlemmar i Europarådet kan ansluta sig till konventionen. Konventionen har ratificerats av Australien, Dominikanska republiken, Japan och USA och undertecknats av Kanada och Sydafrika.

Sverige undertecknade konventionen samma dag som den upprättades, men har ännu inte ratificerat den.

Under arbetet med konventionen fanns det några frågor som inte hann slutbehandlas. Dessa har tagits upp i ett tilläggsprotokoll till konventionen (ETS nr 189).

Tilläggsprotokollet behandlar kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem.

Tilläggsprotokollet öppnades för undertecknande den 28 januari 2003 och trädde i kraft den 1 mars 2006. Hittills (per den 20 maj 2013) har 37 stater undertecknat tilläggsprotokollet och 20 stater ratificerat det.

Sverige undertecknade tilläggsprotokollet samma dag som det upprättades, men har ännu inte ratificerat det.

Frågan om Sverige bör tillträda konventionen och tilläggsprotokollet samt vilka lagändringar som krävs för ett tillträde har behandlats i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6). I promemorian gjordes bedömningen att Sverige borde tillträda såväl konventionen som tilläggsprotokollet. Enligt promemorian uppfyller inte svensk rätt, främst på straffprocessrättens område, konventionens krav. Promemorian har remissbehandlats. Samtliga remissinstanser som yttrade sig i frågan var positiva till att konventionen och protokollet tillträds. Många remissinstanser pekade dock på behovet av samordning med andra pågående lagstiftningsärenden och anförde att förslaget brast i överskådlighet. Det framfördes också att förslag som närmare ansluter till konventionens systematik borde övervägas. Sedan promemorian skrevs har förutsättningarna för bedömningen av om svensk rätt uppfyller konventionens krav väsentligen förändrats.

Mot den angivna bakgrunden ingår det i vårt uppdrag att se över vilka författningsändringar som behövs för att Sverige ska kunna leva upp till kraven i konventionen och tilläggsprotokollet.

Den 3 december 1998 antogs i Wien en handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättandet av ett område med frihet, säkerhet och rättvisa. I handlingsplanen angavs i punkten 46 att Europeiska unionen bör vidta åtgärder för att, om det anses nödvändigt, fastställa minimiregler avseende brottsrekvisit och påföljder på bl.a. områdena terrorism och organiserad brottslighet. I handlingsplanen nämndes vidare databrott.

Den 15–16 oktober 1999 höll Europeiska rådet ett särskilt möte i Tammerfors om skapandet av ett område med frihet, säkerhet och rättvisa i unionen. Europeiska rådet förklarade då att insatserna för att enas om gemensamma definitioner, brottsbeskrivningar och påföljder i ett första skede bör begränsas till ett antal sektorer med särskild betydelse, däribland högteknologisk brottslighet.

Vid Europeiska rådets möte i Santa Maria da Feira den 19–20 juni 2000 godkände Europeiska rådet en övergripande handlingsplan för Europa. Handlingsplanen innefattade åtgärder för att förbättra säkerheten på internet och skapa en samordnad och enhetlig strategi för bekämpande av databrottslighet.

Under 2000 offentliggjorde Europeiska kommissionen ett meddelande med titeln ”Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet” (KOM [2000] 890 slutlig). I meddelandet föreslogs en strategi för att bekämpa problemen med databrottslighet. I ytterligare ett meddelande från kommissionen 2001 med rubriken ”Nät- och informationssäkerhet: förslag till en europeisk strategi” analyserades problem rörande nätsäkerhet och presenterades också en strategisk plan för åtgärder inom området (KOM [2001] 298 slutlig). I de båda kommissionsmeddelandena angavs att det finns behov av en snabb tillnärmning av den materiella straffrätten i EU när det gäller angrepp mot informationssystem. Det sistnämnda meddelandet följdes upp med rådets resolution av den 28 januari 2002 om nät- och informationssäkerhet.

I två resolutioner från Europaparlamentet den 19 maj 2000 respektive den 5 september 2001 behandlades också problem med informationssäkerhet och högteknologisk brottslighet.

I ett meddelande den 30 oktober 2001 (KOM [2001] 628 slutlig) angav kommissionen att den avsåg att lägga fram ett förslag till rambeslut om gemensamma definitioner, brottsbeskrivningar och påföljder för angrepp mot informationssystem. Våren 2002 presenterade kommissionen förslaget till rambeslut om angrepp mot informationssystem. Under delar av 2002 och 2003 framförhandlades innehållet i rambeslutet om angrepp mot informationssystem. Vid rådet för rättsliga och inrikes frågor den 27–28 februari 2003 nåddes en politisk överenskommelse om innehållet i rambeslutet. Det antogs sedan den 24 februari 2005. Europarådets konvention om it-relaterad brottslighet har till stor del utgjort förebild för rambeslutet.

Behovet av lagändringar för att genomföra rambeslutet övervägdes i propositionen 2006/07:66 *Angrepp mot informationssystem.*

I propositionen gjordes bedömningen att det för att Sverige fullt ut skulle uppfylla åtagandena enligt rambeslutet krävdes ett utvidgat straffansvar i förhållande till gällande rätt på området. Dataintrångsbestämmelsen utvidgades därför till att omfatta dels den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling, dels den som olovligen allvarligt stör eller hindrar användningen av en sådan uppgift. Kriminaliseringen innebar exempelvis att s.k. tillgänglighetsattacker blev straffbara. Vidare förtydligades dataintrångsbestämmelsen och moderniserades språkligt genom att uttrycket ”uppgift som är avsedd för automatiserad behandling” ersatte det tidigare använda upptagningsbegreppet. Ändringarna trädde i kraft den 1 juni 2007.

Inom EU pågår förhandlingar om att ersätta rambeslutet med ett direktiv om angrepp mot informationssystem (Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF). Europarådets konvention om it-relaterad brottslighet har även utgjort förebild för direktivet. Direktivet syftar till att ytterligare närma medlemsstaternas straffrättslagstiftning till varandra på området för angrepp mot informationssystem och att ändra och utöka bestämmelserna i rambeslutet. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna. Förhandlingarna om direktivet är i allt väsentligt slutförda. Det återstår för EU:s institutioner att formellt anta den text som har godkänts av företrädare för rådet och Europaparlamentet (dok. 11399/12). Efter att direktivet antas har medlemsstaterna två år på sig att genomföra det.

Direktivets bestämmelser, i synnerhet på straffrättens område, överensstämmer till stor del med dem som finns i Europarådets konvention om it-relaterad brottslighet. De lagändringar som kan föranledas av direktivet är därför sådana att de sannolikt behövs även för att tillträda konventionen. Mot denna bakgrund och med beaktande av den tid som Sverige har på sig att genomföra direktivet efter att det antas, ingår det i vårt uppdrag att även analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra det kommande men ännu inte formellt antagna direktivet om angrepp mot informationssystem.

4 Innehållet i konventionen, tilläggsprotokollet och direktivet

4.1 Konventionens innehåll i korthet

Europarådets konvention om it-relaterad brottslighet (konventionen) har tre huvudsyften. Det första är att åstadkomma en tillnärmning av ländernas nationella straffrätt beträffande vissa gärningar. Det andra är att säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser behoven av att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta till vara bevisning i elektronisk form. Det tredje är att lägga grunden för ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott.

I konventionens preambel erinras om behovet av att säkerställa en lämplig avvägning mellan intresset av att lag och ordning upprätthålls och respekten för de grundläggande mänskliga rättigheterna, bl.a. yttrandefriheten och informationsfriheten, så som de garanteras i bl.a. 1950 års Europarådskonvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och 1966 års FN-konvention om medborgerliga och politiska rättigheter.

Konventionen är indelad i fyra kapitel. Dessa innehåller definitioner, bestämmelser om åtgärder som ska vidtas på nationell nivå, bestämmelser om internationellt samarbete och slutbestämmelser.

Konventionstexten i svensk översättning är bifogad betänkandet som *bilaga 3*. Till konventionen har utarbetats en förklarande rapport som finns tillgänglig via bl.a. Europarådets hemsida (www.coe.int). Den förklarande rapporten är vägledande vid tolkningen av konventionen.

Kapitel I – Definitioner

I *artikel 1 a–d* finns definitioner av vissa centrala begrepp som ska gälla vid tillämpningen av konventionen. De begrepp som definieras är *datorsystem*, *datorbehandlingsbara uppgifter*, *tjänsteleverantör* och *trafikuppgifter*. Konventionen innehåller inget krav på att definitionerna ska införas i nationell rätt så länge det finns adekvata motsvarigheter där.

Kapitel II – Åtgärder som ska vidtas på nationell nivå

I kapitel II är bestämmelserna uppdelade i tre avsnitt. I avsnitt 1, som omfattar artiklarna 2–13, finns straffrättsliga bestämmelser, i avsnitt 2, som omfattar artiklarna 14–21, finns processrättsliga bestämmelser och i avsnitt 3 finns artikel 22, som gäller domsrätt.

Avsnitt 1 inleds med artiklar som innehåller krav på kriminalisering av vissa gärningar (artiklarna 2–10). I samtliga dessa bestämmelser är det en förutsättning att gärningen har begåtts uppsåtligen. Vidare är det en förutsättning att det handlande som beskrivs har begåtts ”orättmätigt” (”without right”). Syftet med detta är att markera att ett visst förfarande, som formellt faller in under beskrivningen av vad som ska 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 ”orättmätigt” ska tolkas måste bestämmas med utgångspunkt i det sammanhang där uttrycket förekommer och de principer som gäller i den nationella rätten.

Enligt *artikel 2* ska intrång i hela eller en del av ett 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 mot ett datorsystem som är kopplat till ett annat datorsystem.

Enligt *artikel 3* ska avlyssning med tekniska hjälpmedel av icke allmänna överföringar av datorbehandlingsbara uppgifter till, från eller inom ett datorsystem, inklusive elektromagnetiska emissioner från ett datorsystem med sådana datorbehandlingsbara uppgifter, kriminaliseras. Som villkor för kriminalisering får uppställas krav på

att brottet har begåtts med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Enligt *artikel 4* ska datastörning som består i att någon skadar, raderar, försämrar, ändrar eller undertrycker datorbehandlingsbara uppgifter kriminaliseras. Kriminaliseringen får inskränkas till gärningar som medför allvarlig skada.

Enligt *artikel 5* ska systemstörning som består i att någon allvarligt hindrar ett datorsystems drift genom att mata in, överföra, skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter kriminaliseras.

Artikel 6 anger att viss befattning med olika typer av verktyg ska utgöra ett brott, om gärningen begås i syfte att brott enligt artiklarna 2–5 ska begås.

I *artikel 7* behandlas datorrelaterad förfalskning. Kriminaliseringen ska 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 ska användas för rättsliga ändamål som om de vore autentiska. Som villkor för straffansvar får uppställas krav på bedrägligt uppsåt eller liknande brottsligt uppsåt.

Datorrelaterat bedrägeri regleras i *artikel 8*. Kriminaliseringen ska omfatta att någon förorsakar en annan person förlust av egendom genom att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter eller genom att störa ett datorsystems drift. En förutsättning för straffansvar ska vara att gärningen begås med bedrägligt eller annat brottsligt uppsåt att skaffa en ekonomisk förmån åt sig själv eller någon annan.

Artikel 9 reglerar barnpornografibrott. De handlingar som ska kriminaliseras är bl.a. att på olika sätt med hjälp av datorsystem framställa, bjuda ut eller tillgängliggöra, sprida eller överföra, anskaffa och inneha barnpornografi. 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, och realistiska bilder som föreställer en minderårig som ägnar sig åt sådant handlande.

Enligt *artikel 10* ska olika former av intrång i upphovsrätt och till upphovsrätten närstående rättigheter straffbeläggas, om de begås i kommersiell skala och med hjälp av ett datorsystem. De upphovsrätter som avses i artikeln anges genom en hänvisning till vissa upphovsrättsliga konventioner.

I *artikel 11* regleras försök och olika former av medhjälp till brott.

Enligt *artikel 12* åtar sig konventionsstaterna att under vissa förhållanden ställa juridiska personer till ansvar.

Artikel 13 innehåller bestämmelser om påföljder och åtgärder. Varje konventionsstat ska se till att de brott som föreskrivs i konventionen beläggs med effektiva, proportionella och avskräckande påföljder. De juridiska personer som kan ställas till ansvar enligt artikel 12 ska på motsvarande sätt kunna bli föremål för effektiva, proportionella och avskräckande brottspåföljder eller andra sanktioner.

De processrättsliga reglerna i avsnitt 2 inleds med allmänna bestämmelser som är gemensamma för hela det processrättsliga avsnittet (artiklarna 14 och 15). Härefter följer bestämmelser om skyndsamt säkrande av lagrade uppgifter (artiklarna 16 och 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 ska 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 i elektronisk form. Tillämpningsområdet är således betydligt vidare än enbart de brott som konventionen tar upp.

Rättssäkerhetsgarantier och andra villkor behandlas i *artikel 15*.

Enligt *artikel 16* ska det vara möjligt att genom förelägganden eller på liknande sätt åstadkomma skyndsamt säkrande av särskilt angivna datorbehandlingsbara uppgifter, däribland trafikuppgifter.

Enligt *artikel 17* ska, i fråga om trafikuppgifter som ska säkras enligt artikel 16, sådant säkrande kunna åstadkommas även om flera tjänsteleverantörer har deltagit vid överföringen av meddelandet. I detta syfte ska det vara möjligt att se till att en tillräcklig mängd trafikuppgifter skyndsamt röjs för myndigheterna, så att de tjänsteleverantörer som har deltagit vid överföringen ska kunna identifieras.

Enligt *artikel 18* ska en person kunna föreläggas 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. Vidare ska en tjänsteleverantör kunna föreläggas att lämna ut abonnentuppgifter.

I *artikel 19* regleras husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter. Det ska bl.a. vara möjligt att vid en hus-

rannsakan av ett visst datorsystem skyndsamt utvidga husrannsakan till ett annat datorsystem, om det finns anledning att tro att den information som eftersöks finns i det andra systemet. Vidare ska 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 husrannsakan.

I *artikel 20* regleras insamling i realtid av trafikuppgifter.

Artikel 21 reglerar avlyssning av innehållsuppgifter. Konventionsstaterna åtar sig att i fråga om vissa allvarliga brott, som bestäms i den nationella lagstiftningen, kunna insamla eller ta upp innehållet i särskilt angivna meddelanden, som överförs med hjälp av datorsystem.

I avsnitt 3, som enbart innehåller *artikel 22*, finns regler om domsrätt.

Kapitel III – Internationellt samarbete

Bestämmelserna om internationellt samarbete utgör en betydande del av konventionen. Kapitlet är uppdelat i två avsnitt: ett allmänt avsnitt där de grundläggande principerna för samarbetet läggs fast (artiklarna 23–28) och ett med särskilda bestämmelser om rättslig hjälp med olika former av åtgärder (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 ska 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.

Utlämning behandlas i *artikel 24*. Artikeln reglerar endast utlämning i de fall där det inte finns ett utlämningsavtal mellan staterna eller om staterna, trots att det finns ett sådant avtal, väljer att helt eller delvis använda bestämmelserna i artikeln i stället. Vidare regleras enbart utlämning för brott som anges i artiklarna 2–11.

De allmänna principerna för rättslig hjälp behandlas i *artikel 25*. Konventionsstaterna ska i största möjliga utsträckning ge varandra hjälp för att utreda och lagföra brott som är it-relaterade samt för att samla in bevis i elektronisk form om brott. Artikeln innehåller också detaljregler om kommunikationen mellan parterna.

I *artikel 26* finns bestämmelser om informationsutbyte på eget initiativ, dvs. informationsutbyte som inte sker med anledning av en ansökan om rättslig hjälp eller annan framställning.

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 ska tillämpas.

Av *artikel 27* framgår bl.a. att parterna ska peka ut en eller flera centralmyndigheter som ska ansvara för att sända och ta emot framställningar om rättslig hjälp, verkställa sådana framställningar eller lämna över framställningarna till rätt myndighet. Centralmyndigheterna ska kommunicera direkt med varandra.

Rättslig hjälp ska som huvudregel ges i enlighet med det förfarande som anges av den ansökande staten.

I *artikel 28* finns bestämmelser om sekretess och användningsbegränsning.

I *artikel 29* regleras rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter. En konventionsstat får anmoda en annan konventionsstat att genom föreläggande eller på annat sätt skyndsamt säkra uppgifter som lagrats med hjälp av ett datorsystem inom dennas territorium och vilka den ansökande staten avser att begära rättslig hjälp med åtkomst till. Säkrandet ska 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 ska 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, ska den anmodade staten enligt *artikel 30* skyndsamt för den ansökande staten röja en tillräcklig mängd trafikuppgifter för att tjänsteleverantören i fråga och den väg som meddelandet har överförts ska kunna identifieras.

Artiklarna 31–34 behandlar ömsesidig hjälp med utredningsbefogenheter.

Enligt *artikel 31* får en konventionsstat 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 staten, bl.a. uppgifter som har säkrats enligt artikel 29.

Åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga eller som är åtkomliga med stöd av samtycke behandlas i *artikel 32*. En konventionsstat 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 ska en konventionsstat, genom ett datorsystem inom det egna territoriet, kunna skaffa sig åtkomst till eller ta emot sådana lagrade datorbehandlingsbara uppgifter som finns hos en annan konventionsstat, 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 i realtid av trafikuppgifter. Konventionsstaterna ska lämna rättslig hjälp med insamling i realtid av trafikuppgifter rörande sådana särskilt angivna meddelanden som överförs med hjälp av datorsystem inom staternas territorium. För hjälpen ska gälla de villkor och förfaranden som anges i den nationella rätten. Rättslig hjälp ska dock åtminstone omfatta sådana brott för vilka trafikuppgifter skulle kunna samlas in i realtid i ett motsvarande nationellt förfarande.

I *artikel 34* behandlas rättslig hjälp med avlyssning av innehållsuppgifter i särskilt angivna meddelanden. Konventionsstaterna åtar sig att, så långt den nationella lagstiftningen och tillämpliga överenskommelser medger det, tillhandahålla rättslig hjälp med sådan avlyssning.

Enligt *artikel 35* ska 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 om brott.

Kapitel IV – Slutbestämmelser

I det avslutande kapitlet finns ett antal bestämmelser av formell karaktär.

I *artikel 36* regleras frågan om undertecknande och ikraftträdande.

I *artikel 37* föreskrivs ordningen för hur stat som inte är medlem i Europarådet och som inte har deltagit i utarbetandet av konventionen kan ansluta sig till den.

I *artikel 38* ges en konventionsstat möjlighet att ange för vilket eller vilka territorier konventionen ska gälla.

Artikel 39 behandlar konventionens verkan bl.a. i relation till andra internationella instrument.

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

Artikel 41 behandlar federala stater.

Artikel 42 behandlar uttömmande rätten för konventionsstater att göra förbehåll. Enligt *artikel 43* kan ett förbehåll enligt artikel 42 återtas helt eller delvis.

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

Hur tvister angående tolkningen av konventionen ska lösas anges i *artikel 45*.

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 insamling av bevis i elektronisk form.

Rätten till uppsägning av konventionen behandlas i *artikel 47*.

Artikel 48, slutligen, anger de meddelanden (om undertecknande, deponering av olika instrument, ikraftträdande osv.) som ska lämnas från Europarådets generalsekreterare till bl.a. de fördragsslutande staterna.

4.2 Tilläggsprotokollets innehåll i korthet

Tilläggsprotokollet till konventionen om it-relaterad brottslighet behandlar frågor om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som begåtts med hjälp av ett datorsystem. Protokollet har två syften. Det ena är att åstadkomma en tillnärm-

ning av den materiella straffrätten i fråga om de nämnda brotten. Det andra är att förbättra det internationella samarbetet vid bekämpning av sådana brott.

I protokollets preambel 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.

Tilläggsprotokollet är, liksom konventionen, indelad i fyra kapitel. Dessa innehåller gemensamma bestämmelser, bestämmelser om åtgärder som ska vidtas på nationell nivå, bestämmelser om förhållandet mellan konventionen och tilläggsprotokollet samt slutbestämmelser.

Protokollstexten i svensk översättning är bifogad betänkandet som *bilaga 4*. Till tilläggsprotokollet har, på samma sätt som till konventionen, utarbetats en förklarande rapport som finns tillgänglig via bl.a. Europarådets hemsida (www.coe.int).

Kapitel I – Gemensamma bestämmelser

I *artikel 1* anges syftet med tilläggsprotokollet, som är att komplettera bestämmelserna i konventionen vad gäller kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna 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 ska tolkas på samma sätt som i konventionen.

Kapitel II – Åtgärder som ska vidtas på nationell nivå

Kapitel II innehåller bestämmelser med krav på kriminalisering av vissa gärningar. I samtliga dessa bestämmelser är det en förutsättning att gärningen har begåtts uppsåtligen. På samma sätt som i konventionen är det vidare en förutsättning att det handlande som beskrivs har begåtts ”orättmätigt” (”without right”). 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 ska vara straffbara på försöksstadiet.

Enligt *artikel 3* ska konventionsstaterna straffbelägga gärningar som består i att till allmänheten sprida eller på annat sätt göra tillgängligt rasistiskt och främlingsfientligt material med hjälp av datorsystem. En konventionsstat 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 finns en möjlighet att förbehålla sig rätten att inte tillämpa artikeln i sådana fall av diskriminering där det, på grund av etablerade principer om yttrandefrihet i statens rättssystem, inte kan föreskrivas åtgärder.

I *artikel 4* behandlas hot som är rasistiskt och främlingsfientligt motiverade. Konventionsstaterna ska 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 statens nationella lagstiftning är ett allvarligt brott.

Artikel 5 handlar om kränkningar som är rasistiskt eller främlingsfientligt motiverade. Kriminaliseringen ska 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 konventionsstat 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 konventionsstat ska

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 ska vara fråga om 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 ska kunna förnekas, förringas, förhärligas eller rättfärdigas.

En konventionsstat 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 på grund av ras, hudfärg, härstamning eller nationellt eller etniskt ursprung eller trosbekännelse eller att förbehålla sig rätten att helt eller delvis inte tillämpa artikeln.

Enligt *artikel 7* ska uppsåtlig medhjälp till brott som straffbeläggs i enlighet med protokollet kriminaliseras.

Kapitel III – Förhållandet mellan konventionen och tilläggsprotokollet

I *artikel 8*, som behandlar förhållandet mellan konventionen och tilläggsprotokollet, föreskrivs att följande artiklar i konventionen i tillämpliga delar ska 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, och
- artikel 46 om samråd mellan parterna.

Vidare ska de fördragsslutande staterna utvidga tillämpningsområdet för konventionens processrättsliga bestämmelser (artiklarna 14–21) och bestämmelser om internationellt samarbete (artiklarna 23–35) till att gälla även artiklarna 2–7 i protokollet.

Kapitel IV – Slutbestämmelser

I det avslutande kapitlet finns, liksom i konventionens avslutande kapitel, ett antal bestämmelser av formell karaktär.

Artikel 9 behandlar frågor om undertecknande. Protokollet står öppet för undertecknande av alla som har undertecknat konventionen. Det är alltså 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 den fördragsslutande staten förklarar något annat. I artikeln anges vidare i vilken utsträckning staterna får förklara att de utnyttjar möjligheten att ställa upp särskilda rekvisit. Slutligen anges att en stat har möjlighet att göra förbehåll enligt två artiklar i konventionen, nämligen artikel 22.2 och artikel 41.1, 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*. Meddelanden angående protokollet behandlas i *artikel 16*.

4.3 Direktivets innehåll i korthet

Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF syftar till att ytterligare närma medlemsstaternas strafflagstiftning till varandra på området för angrepp mot informationssystem. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna.

I direktivets preambel uttalas bl.a. att angrepp mot informationssystem, särskilt angrepp som är kopplade till organiserad brottslighet, är ett växande problem både inom unionen och på global

nivå, och att oron ökar för terroristattacker eller politiskt motiverade angrepp mot de informationssystem som ingår i medlemsstaternas och unionens kritiska infrastruktur. Mot bakgrund av att detta utgör ett hot mot arbetet för att skapa ett säkrare informationssamhälle och ett område med frihet, säkerhet och rättvisa understryks behovet av motåtgärder på unionsnivå och bättre samordning och samarbete på internationell nivå. Vidare uttalas att direktivet särskilt syftar till att sörja för att grundläggande friheter och rättigheter – bl.a. de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna – respekteras fullt ut.

Tyngdpunkten i direktivet utgörs av materiella straffrättsliga bestämmelser. De straffrättsliga bestämmelserna överensstämmer till stor del med dem som finns i konventionen och i rådets rambeslut 2005/222/RIF om angrepp mot informationssystem, av vilket det senare alltså ersätts med direktivet.

Som nämnts i avsnitt 3 är direktivet ännu inte formellt antaget, men förhandlingarna om det är i allt väsentligt slutförda. Det återstår för EU:s institutioner att formellt anta den text som har godkänts av företrädare för rådet och Europaparlamentet (dok. 11399/12). En svensk version av denna text är bifogad betänkandet som *bilaga 5*.

I *artikel 1* anges syftet med direktivet, nämligen att fastställa minimiregler när det gäller definitionen av vad som ska utgöra brott och vilka påföljder som ska följa på brotten på området angrepp mot informationssystem. Syftet är också att underlätta förebyggande av sådan brottslighet och att förbättra samarbetet mellan myndigheter som verkar inom området.

I *artikel 2* finns definitioner av vissa centrala begrepp som ska gälla vid genomförandet av direktivet. De begrepp som definieras är *informationssystem*, *datorbehandlingsbara uppgifter*, *juridisk person* och *orättmätigt.* Definitionerna överensstämmer i många delar med de definitioner som finns i artikel 1 i rambeslutet och i artikel 1 i konventionen. Direktivet innehåller inget krav på att definitionerna ska införas i nationell rätt.

I artiklarna 3–7 behandlas vilka gärningar som ska utgöra brott, om de utförs uppsåtligen och orättmätigt.

Enligt *artikel 3* ska intrång i hela eller en del av ett informationssystem vara straffbart när brottet begås genom intrång i en säkerhetsåtgärd. Ringa fall behöver dock inte straffbeläggas.

Av *artikel 4* följer att det ska vara straffbart att 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, åtminstone i fall som inte är ringa.

Enligt *artikel 5* ska det vara straffbart att radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, åtminstone i fall som inte är ringa.

Enligt *artikel 6* ska avlyssning med tekniska hjälpmedel av icke-offentliga överföringar av datorbehandlingsbara uppgifter till, från eller inom ett informationssystem, inklusive elektromagnetisk strålning från informationssystem som innehåller sådana uppgifter, straffbeläggas, åtminstone i fall som inte är ringa.

Artikel 7 anger att viss befattning med olika typer av verktyg ska utgöra ett brott, om gärningen begås i syfte att brott enligt artiklarna 3–6 ska begås, åtminstone i fall som inte är ringa.

I *artikel 8* anges att anstiftan av och medhjälp till sådana gärningar som utgör brott enligt direktivet ska straffbeläggas. Det anges även att brotten olaglig systemstörning och olaglig datastörning i artikel 4 respektive 5 ska straffbeläggas på försöksnivå.

Artikel 9 innehåller både generella och artikelspecifika bestämmelser om vilka påföljder som ska kunna dömas ut för brotten i direktivet. Enligt *artikel 9.1* ska brotten i direktivet generellt ha påföljder som är effektiva, proportionerliga och avskräckande. Enligt *artikel 9.2* ska samtliga brott i direktivet, undantaget osjälvständiga brottsformer och ringa brott, ha en straffskala med ett maximistraff på minst två års fängelse. För brotten olaglig systemstörning (artikel 4) och olaglig datastörning (artikel 5) krävs enligt *artikel 9.3* dessutom ett lägsta maximistraff på tre års fängelse när ett betydande antal informationssystem har påverkats genom användning av ett verktyg som har utformats eller anpassats primärt för detta syfte. För brotten olaglig systemstörning och olaglig datastörning ställs vidare enligt *artikel 9.4* ett krav på ett lägsta maximistraff på fängelse i fem år under tre alternativa förutsättningar: (a) brottet har begåtts inom ramen för en kriminell organisation, (b) brottet har orsakat allvarlig skada, eller (c) brottet har begåtts mot ett kritiskt infrastrukturinformationssystem. *Artikel 9.5* anger att missbruk av andra personers personuppgifter ska utgöra en försvårande omständighet vid brotten olaglig systemstörning och olaglig datastörning när det innebär olägenheter för denna person i

den mån detta missbruk inte redan täcks av andra brott i den nationella lagstiftningen.

Artikel 10 har under förhandlingarna utgått ur utkastet till direktiv.

I *artiklarna 11* och *12* regleras juridiska personers ansvar samt påföljder för juridiska personer.

Jurisdiktionsfrågor regleras i *artikel 13*.

I *artikel 14* finns bestämmelser om informationsutbyte, som bl.a. innebär att medlemsstaterna ska peka ut en operativ nationell kontaktpunkt som kan nås dygnet runt alla dagar i veckan.

I *artikel 15* finns bestämmelser om övervakning och statistik.

Direktivet avslutas med bestämmelser om ersättande av 2005 års rambeslut (*artikel 16*), införlivande (*artikel 17*), rapporteringsskyldighet (*artikel 18*), ikraftträdande (*artikel 19*) och adressater (*artikel 20*).

5 Behovet av lagändringar mot bakgrund av konventionen

5.1 Inledning

I vårt uppdrag ingår att analysera behovet av författningsändringar för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet (konventionen) med tilläggsprotokoll. Vi ska också lämna förslag till de författningsändringar som behövs för att möjliggöra ett svenskt tillträde till instrumenten. I detta kapitel analyseras med utgångspunkt i konventionens artiklar de behov av lagändringar som konventionen föranleder. I följande kapitel görs motsvarande analys i förhållande till tilläggsprotokollet.

5.2 Definitioner (artikel 1)

I *artikel 1* finns definitioner av centrala termer som ska gälla vid tillämpning av konventionen. Det ställs inte något krav på att definitionerna ska införas i nationell rätt.

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. I svenskt språkbruk torde den lämpligaste termen för det som åsyftas i konventionen vara ”datasystem”. Enligt Svenska datatermgruppens ordlista (ord-

listeartikel 64) innefattas nämligen i detta begrepp datorer, program, servrar m.m. liksom den tekniska lösningen och utformningen.

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 (se dock artikel 3). Definitionen avser data i elektronisk eller annan 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 för användarna av en sådan tjänst. Det saknar betydelse om det är fråga om öppna eller slutna nätverk.

I lagen (2003:389) om elektronisk kommunikation (LEK) definieras ”*operatör*” som den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation (1 kap. 7 §). Konventionens definition av tjänsteleverantör är alltså vidare än LEK:s definition av operatör. Begreppet tjänsteleverantör i konventionens mening omfattar enligt vår bedömning i huvudsak den krets av aktörer som på flera ställen i LEK benämns som ”den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst” (se 6 kap. 20 och 22 §§ LEK). Vi kommer fortsättningsvis att använda oss av begreppet ”leverantör” när vi åsyftar en vidare personkrets än den som omfattas av LEK:s definition av operatör. I sammanhanget kan dock påpekas att regleringen i LEK i fråga om vilka tjänster och nät som omfattas av lagen och vilka skyldigheter som gäller för olika aktörer inte är lättöverskådlig.

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 hänför 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).

5.3 Straffrättsliga bestämmelser

5.3.1 Allmänt om bestämmelserna

Konventionens straffrättsliga bestämmelser omfattar brott som är direkt riktade mot datorbehandlingsbara uppgifter och datorsystem (artiklarna 2–6), datorrelaterade brott (artiklarna 7 och 8), innehållsrelaterade brott (artikel 9), och brott mot upphovsrätt m.m. (artikel 10) samt försök och medhjälp till de nämnda brotten (artikel 11). Konventionen behandlar enbart *uppsåtliga* brott. I samtliga artiklar, utom artikeln som gäller upphovsrätt, finns dessutom krav på att gärningen ska ha begåtts *orättmätigt* (”without right”). Syftet med detta är, som nämnts i avsnitt 4.1, att ange att ett visst handlande, trots att det faller in under beskrivningen av vad som ska vara kriminaliserat, ändå kan vara tillåtet. Det kan till exempel stödjas på lag, medgivande, avtal eller omständigheter som utesluter straffansvar enligt den nationella rätten. Vad som ska läggas i begreppet orättmätigt får avgöras utifrån det sammanhang där det förekommer (se den förklarande rapporten p. 38).

Ringa brott får, utan att det har kommit till direkt uttryck i konventionstexten, undantas från kriminalisering (se den förklarande rapporten p. 37).

5.3.2 Den svenska dataintrångsbestämmelsen och motsvarande bestämmelser i Finland, Danmark och Norge

När det gäller frågan om svensk rätt uppfyller konventionens krav är den svenska bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken av central betydelse för flera av konventionens straffrättsliga artiklar. I detta avsnitt görs därför en genomgång av bestämmelsen om dataintrång.

Bestämmelsen om dataintrång infördes i brottsbalken 1998 i samband med att den tidigare datalagen (1973:289) ersattes med personuppgiftslagen (1998:204). Datalagens bestämmelse om dataintrång (21 §) överfördes då till brottsbalken utan ändring i sak. Datalagen hade tillkommit samtidigt som vissa ändringar gjorts i tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet. Bestämmelsen om dataintrång fick sin nuvarande utformning genom en lagändring 2007 som i huvudsak syftade till att genomföra EU:s rambeslut 2005/222/RIF om angrepp mot informationssystem.

För *dataintrång* döms den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Straffet är böter eller fängelse i högst två år.

Uttrycket ”uppgift som är avsedd för automatiserad behandling” infördes i bestämmelsen i samband med lagändringen 2007. Det ersatte då det tidigare använda begreppet ”upptagning för automatisk databehandling”. Denna lagändring var inte direkt föranledd av det nämnda rambeslutet utan hade till syfte att förtydliga och språkligt modernisera dataintrångsbestämmelsen. Avsikten med det valda begreppet är att fånga in alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form och att även program av olika slag ska omfattas av begreppet (prop. 2006/07:66 s. 40 och 49). För tillämpningen av begreppet ska det vara utan betydelse var någonstans de nämnda uppgifterna finns eller förvaras i systemet och det ska inte längre finnas något utrymme för diskussioner om uppgifterna är att anse som ”fixerade” eller inte, på vilket datamedium de förvaras eller med vilken teknik de överförs (prop. 2006/07:66 s. 40–41). Även uppgifter som finns i en dators temporära minne omfattas och vidare också uppgifter som är under befordran, oavsett på vilket sätt befordran sker (prop. 2006/07:66 s. 49). När det gäller uppgifter som befordras via radio sägs emellertid i propositionen att avlyssning av sådan radiokommunikation faller utanför det straffbara området eftersom det följer av principen om att etern är fri och av att olovlighetsrekvisitet (se närmare i det följande) därmed inte kan anses uppfyllt (prop. 2006/07:66 s. 49). Om intrånget däremot sker i radiobefordrade uppgifter som t.ex. är krypterade anges i propositionen att ansvar för dataintrång dock kan komma i fråga och att sådant ansvar också kan komma i fråga för ändring eller utplånande av eller annan påverkan på radiobefordrade uppgifter som anges i paragrafen (prop. 2006/07:66 s. 49).

Ansvar för dataintrång förutsätter *uppsåt* (1 kap. 2 § brottsbalken). Gärningsmannen behöver inte handla med ett direkt uppsåt att åstadkomma viss effekt utan alla uppsåtsformer, även likgiltighetsuppsåt, är tillämpliga (Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 4:50 c). För straffansvar krävs vidare att gärningen utförs *olovligen*. Härmed utesluts från det straffbara området sådant förfarande som sker med samtycke av den som har rätt att förfoga

över uppgiften eller i överensstämmelse med gällande rätt, t.ex. regler om tvångsmedel (jfr Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 4:50 c).

Det handlande som straffbeläggs i dataintrångsbestämmelsen är för det första att någon *bereder sig tillgång till* en uppgift som är avsedd för automatiserad behandling. Det krävs inte att det sker i ett visst syfte eller att det medför någon särskild effekt, t.ex. skada. Inte heller förutsätts att någon säkerhetsåtgärd kringgås. Vidare straffbeläggs att *ändra*, *utplåna* eller *blockera* en sådan uppgift som nyss angetts. En ändring kan direkt gälla den uppgift som ska databehandlas. En ändring kan också göras i det datorprogram som styr den aktuella databehandlingen. Ändringen kan vara bestående eller tillfällig (Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 4:50 a). Att en uppgift utplånas innebär att den helt eller delvis förstörs, t.ex. genom radering. Att dataintrångsbestämmelsen även omfattar den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling infördes år 2007 som en följd av anpassningen till det tidigare nämnda rambeslutet från 2005. Med ”blockera” ska förstås åtgärder som innebär att en uppgift görs oåtkomlig eller hindras från att flöda. Det ska alltså handla om hindrande eller spärrande åtgärder av olika slag (prop. 2006/07:66 s. 50). Som exempel på åtgärder nämns i propositionen inmatning eller spridning av olika typer av sabotageprogram, t.ex. datavirus, trojaner eller logiska bomber.

Det är vidare också straffbelagt som dataintrång att *föra in* en uppgift som är avsedd för automatiserad behandling *i ett register*. Registerbegreppet medför en begränsning av det straffbara området så till vida att endast sådana införingar som sker i uppgifter strukturerade på visst sätt omfattas. Således omfattar tillämpningsområdet för dataintrångsbestämmelsen i denna del inte alla slag av införingar av uppgifter. Andra införingar kan dock vara straffbara genom att de träffas av de delar av bestämmelsen som straffbelägger ändring eller utplånande av samt intrång i uppgifter.

Slutligen omfattar dataintrångsbestämmelsen även den som olovligen genom någon annan liknande åtgärd än de som redovisats ovan *allvarligt stör eller hindrar användningen av* en uppgift som är avsedd för automatiserad behandling. Även denna del av bestämmelsen tillkom till följd av anpassningen till rambeslutet. Det straffbara förfarandet tar sikte på åtgärder som verkar på ett sådant sätt att de stör eller hindrar att uppgifter som är avsedda för automatiserad behandling kan användas på avsett sätt, dvs. åtgärder som påverkar

driften av ett system och därmed också användningen av de uppgifter som finns i systemet utan att uppgifterna helt blockeras (prop. 2006/07:66 s. 43–44 och 50). Som exempel på sådana åtgärder nämns i propositionen tillgänglighetsattacker eller överbelastningsattacker och anges att det t.ex. kan handla om program som skapar och sänder så stora mängder e-post att mottagarens system kollapsar eller får kraftigt nedsatt funktion och därmed hindrar eller stör användningen av de uppgifter som finns i systemet (prop. 2006/07:66 s. 50). Som ytterligare exempel på åtgärder som kan verka på ett sådant sätt nämns i propositionen upprepade anrop eller försök till anrop, införing av virusprogram eller annat sabotageprogram.

Bestämmelsen om dataintrång är subsidiär i förhållande till straffbestämmelserna om brytande av post- eller telehemlighet i 4 kap. 8 § brottsbalken och om intrång i förvar i 4 kap. 9 § brottsbalken.

Som framgått av det anförda anges det objekt som skyddas i dataintrångsbestämmelsen med begreppet uppgift som är avsedd för automatiserad behandling. Utgångspunkten är alltså att det är *uppgiften* som är det skyddsvärda. På samma sätt utgår bestämmelsen om brytande av post- eller telehemlighet i 4 kap. 8 § brottsbalken från att det är själva *meddelandet* som är det skyddsvärda. Den svenska regleringen skiljer sig i detta avseende till viss del från vissa andra staters, vilkas reglering i större utsträckning i stället tar själva *tillvägagångssättet* som utgångspunkt för den straffrättsliga regleringen. Även konventionens straffrättsliga artiklar är till stor del uppbyggda med utgångspunkt i själva förfarandet.

I *Finland* ska den dömas för *dataintrång* som genom att göra 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 eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system (38 kap. 8 § 1 mom. strafflagen). Brottet fullbordas när personen tar sig igenom systemets skydd och uppgifterna i systemet behöver inte röras på något sätt för att brottet ska fullbordas. Om uppgifterna används eller skadas tillämpas bestämmelser om olovligt brukande eller skadegörelse (28 kap. resp. 35 kap. strafflagen, se den finska regeringens proposition RP 153/2006 rd s. 14). Vidare ska den dömas för dataintrång som utan att tränga in i datasystemet eller en del av detta med tekniska specialanordningar obehörigen tar reda på information som finns i ett sådant datasystem som nyss nämnts (samma bestämmelses 2 mom.). Handlandet förutsätter alltså inte att något egentligt intrång gjorts i

systemet utan dataintrånget görs t.ex. genom att man lagrar och analyserar s.k. elektromagnetiska emissioner från en dator (se den finska regeringens proposition RP 153/2006 rd s. 14).

När det gäller förfaranden som innebär att datorbehandlingsbara uppgifter skadas, raderas, försämras, ändras eller blockeras (jfr artikel 4 i konventionen) straffas de i Finland enligt bestämmelser om *skadegörelse* (35 kap. 1 § strafflagen). För skadegörelse ska den dömas som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning (2 mom. i den nämnda bestämmelsen). Med information som har upptagits på ett datamedium avses såväl informationens sakinnehåll som de tecken som förmedlar sakinnehållet. Med datamedium avses t.ex. dokument, grammofonskivor, film och disketter (se den finska regeringens proposition RP 153/2006 rd s. 16).

Härutöver finns bestämmelser som syftar till allmänt skydd av kommunikation och som täcker exempelvis överbelastningsattacker riktade mot kommunikation. Den som genom att ingripa i en för posttrafik eller för tele- eller radiokommunikationer använd anordningsfunktion, genom att med en radioanläggning eller över ett telenät av okynne sända störande meddelanden eller på något annat motsvarande sätt obehörigen hindrar eller stör posttrafik eller tele- eller radiokommunikationer, ska dömas för *störande av post- och teletrafik* (38 kap. 5 § strafflagen). Bestämmelsens tillämpningsområde begränsar sig alltså till kommunikation, dvs. överföring av meddelanden från ett ställe till ett annat (se den finska regeringens proposition RP 153/2006 rd s. 17). Det finns därför även särskilda bestämmelser om systemstörning (vilka infördes för att tillgodose konventionens krav i artikel 5). För *systemstörning* ska den dömas som i syfte att orsaka en annan person olägenhet eller ekonomisk skada matar in, överför, skadar, ändrar eller undertrycker data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarlig skada i det.

I *Danmark* ska den dömas för ”intrång i datasekretess” (*kraenkelse af datahemmeligheden*) som oberättigat bereder sig tillgång till någon annans uppgifter eller program, som är avsedda att användas i en anläggning för elektronisk databehandling (straffelovens § 263, stk 2). När det gäller förfaranden som innebär att datorbehandlingsbara uppgifter skadas, raderas osv. straffbeläggs de, liksom i Finland, enligt bestämmelser om *skadegörelse* (*haervaerk*). För skadegörelse döms således den som förstör, skadar eller avlägsnar sak som tillhör

någon annan (straffelovens § 291, stk 1). Bestämmelsen anses alltså tillämplig även på sådana åtgärder som innebär att datorbehandlingsbara uppgifter exempelvis skadas eller blockeras (se det danska justitiedepartementets bedömning i Forslag til Lov om aendring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven, Lovforslag nr. L 55, Folketinget 2003–04, s. 43).

Även förfaranden som består i att hindra ett datorsystems drift genom att skada, radera, försämra, ändra eller blockera datorbehandlingsbara uppgifter, anses omfattas av det nämnda skadegörelsebrottet (straffelovens § 291, stk 1).

När det gäller åtgärder som innebär att driften av ett datorsystem hindras genom att datorbehandlingsbara uppgifter matas in eller överförs anses dessa omfattas av en bestämmelse som enligt svensk rätt närmast är att beteckna som *egenmäktigt förfarande* (*rådighetshindring*). Enligt bestämmelsen (straffelovens § 293, stk. 2) straffas den som oberättigat hindrar en annan att helt eller delvis råda över saker. Uttrycket ”oberättigat hindrar” ersatte, i samband med Danmarks tillträde till konventionen, den i bestämmelsen tidigare använda formuleringen ”lägger hinder i vägen” för att precisera att det inte krävs något fysiskt hindrande för att bestämmelsen ska kunna tillämpas och att således också hinder av elektroniskt slag omfattas. Uttrycket ”helt eller delvis” är valt för att precisera att också ett hinder som innebär att den berättigade begränsas väsentligt i sin rådighet omfattas, t.ex. när det är fråga om tillgänglighetsattacker, som bara delvis omöjliggör användningen av ett informationssystem (se författningskommentaren till ändringarna i bestämmelsen i Forslag til Lov om aendring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven, Lovforslag nr. L 55, Folketinget 2003–04, s. 64).

I *Norge* döms den för *dataintrång* (*datainbrudd*) som genom att bryta en säkerhetsåtgärd eller på liknande sätt oberättigat bereder sig tillgång till uppgifter (*data*) eller program (*programutrustning*) som är lagrade eller som överförs med elektroniska eller tekniska hjälpmedel (straffeloven § 145 andra stycket).[1] Med ”uppgifter” avses all slags maskinläsbar information, t.ex. om personliga, tekniska eller ekonomiska förhållanden. Med ”program” avses instruktioner till en datamaskin, alltså dataprogram (se den norska propositionen Ot.prp. nr. 40, [2004–2005] s. 12). I begreppet ”bereda sig tillgång till” ligger inget krav på att personen som gjort intrånget tillägnat

[1] I juni 2009 beslutades om vissa ändringar i den norska dataintrångbestämmelsen och om vissa nya bestämmelser om datakriminalitet. Dessa har emellertid inte trätt i kraft och det är ovisst när de kommer att göra det.

sig informationen utan det är tillräckligt att uppgifterna, genom intrånget, gjorts tillgängliga för honom eller henne (se Datakrimutvalgets betänkande *Lovtiltak mot datakriminalitet*, NOU 2003:27, s. 14). Bestämmelsen om dataintrång anses tillämplig på olika former av avlyssning av datorbehandlingsbara uppgifter och även på avlyssning av elektromagnetisk strålning, om strålningen kan omskapas till logisk information (se Datakrimutvalgets betänkande *Lovtiltak mot datakriminalitet*, NOU 2003:27, s. 16).

När det gäller förfaranden som innebär att datorbehandlingsbara uppgifter skadas, raderas osv. straffbeläggs de, liksom i Finland och Danmark, enligt bestämmelser om *skadegörelse*, varigenom det är straffbart att förstöra eller skada ett föremål (straffeloven § 291). Uppgifterna i sig skyddas i och för sig inte av bestämmelsen men ett medium för lagring av uppgifter är ett sådant föremål som avses i bestämmelsen. En ändring eller radering av uppgifter anses innebära skadegörelse på lagringsmediet eftersom det då inte kan användas på det sätt som är förutsatt (se Datakrimutvalgets betänkande *Lovtiltak mot datakriminalitet*, NOU 2003:27, s. 17). Även åtgärder som innebär att ett datorsystems drift störs anses kunna straffas enligt den nämnda skadegörelsebestämmelsen (se Datakrimutvalgets betänkande *Lovtiltak mot datakriminalitet*, NOU 2003:27, s. 18).

5.3.3 Olagligt intrång (artikel 2)

Bedömning: Svensk rätt uppfyller genom dataintrångsbestämmelsen konventionens krav på vad som ska vara straffbelagt som olagligt intrång. 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 behöver inte uppställas.

Skälen för bedömningen

Enligt *artikel 2* ska orättmätigt intrång i hela eller en del av ett datorsystem vara straffbart, när det görs uppsåtligen. Krav får uppställas 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.

Handlingen kan rikta sig mot antingen *hela* eller *en del av ett datorsystem*. Begreppet *datorsystem* definieras i artikel 1 a som ”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”.

Gärningen ska begås genom *intrång*. Detta innebär att gärningsmannen ska ”komma in i” datorsystemet, och enbart sändande av e-post eller en fil till datorsystemet innebär exempelvis inte intrång i artikelns mening (se den förklarande rapporten p. 46).

Artikeln förutsätter att gärningen begås med *uppsåt* och att den utförs *orättmätigt*. Kravet på att handlingen ska vara orättmätig innebär att handlingar som i och för sig uppfyller övriga krav på straffbarhet men som utförs antingen av eller med tillstånd från ägare eller annars behöriga personer i ett företag i enlighet med behörigheten, t.ex. för att testa datasäkerheten, inte omfattas av det område som ska vara straffbelagt. Inte heller omfattas att bereda sig tillgång till ett datorsystem som tillåter fritt och öppet tillträde, exempelvis att ladda ner internetsidor som är avsedda att vara offentliga (se den förklarande rapporten p. 38 och 47).

Som framgått i avsnitt 5.3.2 straffbelägger den svenska dataintrångsbestämmelsen bl.a. den som uppsåtligen och olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling. Såväl dataintrångsbestämmelsen som artikel 2 förutsätter alltså att gärningen begås med uppsåt. Begreppet orättmätigt i artikel 2 får anses motsvara begreppet olovligen i dataintrångsbestämmelsen. Som vidare framgått var avsikten med införandet av begreppet uppgift som är avsedd för automatiserad behandling i dataintrångsbestämmelsen att förtydliga att alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form, omfattas av bestämmelsen och att även program av olika slag omfattas. Det är för tillämpningen av begreppet utan betydelse var uppgifterna finns eller förvaras i systemet, vilket innebär att alla uppgifter, oavsett på vilket datamedium de finns, omfattas. Således omfattas uppgifter som finns i en dators temporära minne, t.ex. arbetsminnet, och uppgifter som är under befordran, oavsett på vilket sätt befordran sker (med viss reservation för uppgifter som befordras via radio).

För straffansvar för dataintrång är det tillräckligt att någon *bereder sig tillgång till* uppgifter avsedda för automatiserad behandling, dvs.

att personen *kan få del* av dem. Det krävs alltså inte att personen verkligen *tar del* av uppgifterna. Bestämmelsen kan därför vara tillämplig så snart någon olovligen tar sig in i en apparat som används för uppgifter avsedda för automatiserad behandling (se prop. 2006/07:66 s. 24). Genom tillträdet till apparaten har personen skaffat sig möjlighet att ta del av de uppgifter som finns i apparaten och alltså berett sig tillgång till dessa.

Enligt vår bedömning uppfyller svensk rätt, genom dataintrångsbestämmelsen, konventionens krav på vad som ska vara straffbelagt som olagligt intrång. Motsvarande bedömning gjordes i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6, s. 95). Det finns inte anledning att utnyttja rätten att 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.

I sammanhanget bör nämnas att konventionens artikel 2 i huvudsak motsvarar artikel 2 i EU:s rambeslut om angrepp mot informationssystem (Rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem). I den proposition i vilken behovet av lagändringar för att genomföra rambeslutet övervägdes, gjorde regeringen bedömningen att svensk rätt genom dataintrångsbestämmelsen uppfyllde artikelns krav (prop. 2006/07:66 s. 22–24). Vidare bör nämnas att i det kommande EU-direktivet som ska ersätta rambeslutet upptas en bestämmelse om olagligt intrång i informationssystem (artikel 3) som i princip överensstämmer med artikel 2 i rambeslutet, och därmed också med konventionens artikel 2 (se närmare avsnitt 7.3.1).

5.3.4 Olaglig avlyssning (artikel 3)

Bedömning: Svensk rätt uppfyller genom bestämmelsen om brytande av post- eller telehemlighet och dataintrångsbestämmelsen konventionens krav på vad som ska vara straffbelagt som olaglig avlyssning. Krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem behöver inte uppställas vid ett tillträde till konventionen.

Skälen för bedömningen

Enligt *artikel 3* ska det vara straffbart som olaglig avlyssning att uppsåtligen 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. Krav får uppställas på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Begreppet *datorbehandlingsbara uppgifter* definieras i artikel 1 b som ”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” (se under avsnitt 5.2 vad som avses med begreppet *datorsystem*). Redan här bör nämnas att begreppet *uppgift som är avsedd för automatiserad behandling* i dataintrångsbestämmelsen måste anses motsvara vad som enligt konventionen ska förstås med ”datorbehandlingsbara uppgifter” (jfr prop. 2006/07:66 s. 25–26).

Enligt den förklarande rapporten (p. 51) är syftet med bestämmelsen att skydda rätten till privatliv när det gäller datakommunikation. Olaglig avlyssning av datorbehandlingsbara uppgifter utgör enligt rapporten motsvarande kränkning av rätten till privata kommunikationer som traditionell avlyssning och inspelning av telefonsamtal mellan personer (se artikel 8 i Europakonventionen). Enligt rapporten gäller alltså brottet alla former av elektronisk dataöverföring, oavsett om den sker genom telefon, fax, e-post eller filöverföring.

Med att *avlyssna* avses i bestämmelsen att lyssna på eller övervaka innehållet i kommunikation eller att få tillgång till innehållet i uppgifter antingen direkt genom åtkomst till och användande av datorsystemet eller indirekt genom användande av elektronisk avlyssningsutrustning och kan också innefatta inspelning (se den förklarande rapporten p. 53). Bestämmelsen omfattar endast avlyssning med *tekniska hjälpmedel*, vilket är avsett att innebära en begränsning av bestämmelsens räckvidd (se den förklarande rapporten p. 53).

Bestämmelsen träffar enbart *icke allmänna överföringar*. Begreppet ”icke allmän” (*non-public*) avser karaktären av överföringen och inte karaktären av uppgifterna som överförs. Uppgifterna kan alltså bestå av information som är allmänt tillgänglig men avlyssning av dem ändå träffas av bestämmelsen om de som kommunicerar har för avsikt att göra detta förtroligt. Begreppet fångar också upp fall

där informationen är tänkt att vara tillgänglig först när mottagaren har betalt för den, exempelvis vid betal-tv (se den förklarande rapporten p. 54).[2] Kommunikationen, dvs. överföringen av datorbehandlingsbara uppgifter, kan ske mellan *datorer*, mellan *olika delar i en dator* eller mellan *en dator och dess användare* (se den förklarande rapporten p. 55).

Det straffbara handlandet ska, som framgått, omfatta även orättmätig avlyssning av *elektromagnetiska emissioner* från ett datorsystem med datorbehandlingsbara uppgifter. I sammanhanget bör följande nämnas. Genom elektromagnetiska emissioner eller *elektromagnetisk strålning* överförs energi som en vågrörelse av elektriska och magnetiska fält, vilka fortplantas i tid och rum. Vågorna karakteriseras av frekvens, våglängd, utbredningshastighet och polarisation. Exempel på elektromagnetisk strålning är radiovågor, värmestrålning, ljus (exempelvis infrarött ljus) samt röntgen- och gammastrålning. Radiovågor är den mest lågfrekventa formen av elektromagnetisk strålning. I lagen (2003:389) om elektronisk kommunikation (LEK) definieras radiovågor som elektromagnetiska vågor med frekvenser från 9 kilohertz till 3 000 gigahertz som breder ut sig utan särskilt anordnad ledare. Vid trådlös teknik, exempelvis vid användning av trådlösa telefoner och trådlösa datornätverk, skickas signaler med hjälp av radiovågor från en apparat till en annan. I trådlösa datornätverk sänder både routern och datorns nätverkskort radiovågor. Sådan radioöverföring kan ske slutet, dvs. i ett stängt lösenordsförsett nätverk, eller öppet. Kommunikation mellan ett trådlöst tangentbord och en dator sker också vanligtvis via radiokommunikation men det finns även typer som använder infraröd strålning, alltså elektromagnetisk strålning i ett annat frekvensområde än radiovågor. I vart fall om det är fråga om ett bluetooth-tangentbord är kommunikationen oftast krypterad. Även mobiltelefoner och de basstationer som en sådan har kontakt med skickar och tar emot signaler med hjälp av radiovågor.

Enligt den förklarande rapporten (p. 57) kan elektromagnetiska emissioner sändas ut av en dator under drift. Sådana emissioner anses inte vara *uppgifter* enligt konventionens definition av datorbehand-

[2] I svensk rätt är i stort sett all kommersiell hantering av utrustning för olovlig avkodning straffbar genom lagen (2000:171) om förbud beträffande viss avkodningsutrustning. Någon särskild straffrättslig sanktion för privat bruk eller innehav av olovlig avkodningsutrustning finns dock inte. Vår uppfattning är emellertid att detta inte hindrar oss från att tillträda konventionen, eftersom sådana förfaranden som artikel 3 främst avser att straffbelägga är straffbara som brytande av post- eller telehemlighet eller dataintrång, se närmare i det följande.

lingsbara uppgifter i artikel 1 b. Eftersom emissionerna emellertid kan *omskapas till uppgifter* har avlyssning av uppgifter ur elektromagnetiska emissioner tagits med som ett brott i bestämmelsen. Enligt rapporten (p. 56) innebär den omständigheten att begreppet ”datorsystem” också kan omfatta radioförbindelser inte en skyldighet att kriminalisera avlyssning av varje radioöverföring som, även om den inte är ”allmän”, äger rum på ett relativt öppet och lättillgängligt sätt och därför kan avlyssnas av exempelvis radioamatörer.

Gärningen ska vidare begås *orättmätigt*, vilket innebär att bestämmelsen exempelvis inte träffar en myndighet som har laglig rätt att avlyssna för att utreda brott eller den som har fått tillstånd att avlyssna från dem som deltar i överföringen. Inte heller är bestämmelsen tänkt att omfatta användningen av s.k. kakor[3] för att i kommersiella syften följa enskilda användare på webbplatser (se den förklarande rapporten p. 58).

I svensk rätt är det främst bestämmelserna om *brytande av post- eller telehemlighet* (4 kap. 8 § brottsbalken) och *dataintrång* (4 kap. 9 c § brottsbalken) som är relevanta för frågan i vad mån Sverige uppfyller kraven på kriminalisering i artikel 3. Upplysningsvis kan här nämnas att i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att det krävdes lagändringar för att leva upp till konventionens krav på kriminalisering av olaglig avlyssning.[4] Det föreslogs därför att dataintrångsbestämmelsen skulle ändras på visst sätt (Ds 2005:6 s. 217–223).

Innan straffbestämmelserna gås igenom bör emellertid något sägas om *principen om eterns frihet*. Sedan länge har, såväl nationellt som internationellt, ansetts gälla som en grundläggande princip att ”etern är fri”. Detta har ansetts innebära att det i princip är tillåtet för var och en att fritt avlyssna såväl radiokommunikation som är riktad till allmänheten som annan typ av radiokommunikation (se t.ex. prop. 1992/93:200 s. 166, 2002/03:110 s. 254 och 2006/07:66 s. 41). Uppfattningen synes för svenskt vidkommande ha sin främsta grund i ett förarbetsuttalande till 2 kap. 6 § regeringsformen (den nya bestämmelsen 2 kap. 6 § *första stycket* regeringsformen motsvarar i denna del förutvarande bestämmelse, prop. 2009/10:80 s. 249). Av

[3] En kaka (cookie) är en liten textbaserad datafil som en webbserver kan be att få spara i webbplatsbesökarens dator. Kakorna skickas i allmänhet tillbaka med varje förfrågan till den aktuella webbplatsen. Det är därför möjligt för servern att hålla reda på besökarens preferenser eller identitet. Kakor kan användas för statistik, reklam m.m. De kan också användas för att besökaren automatiskt ska få det språk och den textstorlek som denne tidigare har valt.

[4] När bedömningen gjordes var begreppet ”upptagning för automatisk databehandling” i dataintrångsbestämmelsen ännu inte ersatt av det nu använda ”uppgift som är avsedd för automatiserad behandling”, vilket kan ha haft viss betydelse för bedömningen.

2 kap. 6 § första stycket regeringsformen följer att var och en (tidigare ”varje medborgare”) i Sverige är gentemot det allmänna skyddad mot bl.a. kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Av 2 kap. 6 § andra stycket regeringsformen följer dessutom att var och en, utöver vad som föreskrivs i bestämmelsens första stycke, gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (bestämmelsen tillkom i samband med grundlagens reformering, och innebär alltså att skyddet mot intrång i den personliga integriteten har utvidgats, prop. 2009/10:80 s. 250).

Skyddet i 2 kap. 6 § regeringsformen är relativt i den meningen att det under vissa förutsättningar får begränsas genom lag. En sådan begränsning får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får heller inte 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 såsom en av folkstyrelsens grundvalar. Slutligen får en sådan begränsning inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 §, tidigare 2 kap. 12 §, regeringsformen).

Avlyssning av kommunikation mellan enskilda som sker trådlöst, t.ex. via radio eller satellit har inte ansetts omfattas av grundlagsskyddet i 2 kap. 6 § första stycket regeringsformen mot hemlig avlyssning, eftersom detta skydd begränsas till ”förtroliga meddelanden”. I det nämnda förarbetsuttalandet anfördes således att beträffande meddelanden som överbringas under sådana omständigheter att vem som helst kan ta del av dem, t.ex. via samtal i en folksamling eller via radio, kunde någon förtrolighet inte sägas råda (SOU 1975:75 s. 200, prop. 1975/76:209 s. 147).

Resonemanget stöds av bestämmelser i LEK om skydd för hemligheten i elektroniska meddelanden. Enligt 6 kap. 17 § första stycket LEK får inte någon annan än berörda användare ta del av eller på annat sätt behandla uppgifter i ett elektroniskt meddelande som överförs i ett allmänt kommunikationsnät eller med en allmänt tillgänglig kommunikationstjänst, eller trafikuppgifter som hör till detta meddelande, om inte en av användarna har samtyckt till detta. Undantag från förbudet mot att behandla uppgifter görs emellertid för bl.a. den som i radiomottagare har avlyssnat eller på annat sätt med använ-

dande av sådan mottagare fått tillgång till ett radiobefordrat elektroniskt meddelande som inte är avsett för den som avlyssnar eller för allmänheten (andra stycket, p. 3). Enligt 6 kap. 23 § LEK får emellertid den som via en radiomottagare avlyssnat eller på annat sätt med användande av sådan mottagare fått tillgång till ett meddelande som inte är avsett för honom eller henne själv, inte obehörigen föra det vidare. Förbudet är straffsanktionerat (enligt 7 kap. 15 § LEK kan den som med uppsåt eller oaktsamhet bryter mot tystnadsplikten dömas till böter). Mot bakgrund av utgångspunkten om att etern är fri och att var och en anses ha rätt att inneha en radiomottagare har det således inte ansetts vara en framkomlig väg att straffsanktionera själva *avlyssningen* i mottagare av radiomeddelanden (prop. 2002/03:110 s. 254).

I förarbetena (prop. 1992/93:200 s. 166) till telelagen (1993:597) angav regeringen att den huvudsakliga utgångspunkten för den dåvarande regleringen av tystnadsplikten i 3 a § radiolagen (1966:755) för den som i mottagare avlyssnat ett telemeddelande var att etern är fri och att envar enligt radiolagstiftningen i princip fritt kan lyssna till radiobefordrade meddelanden. Regeringens bedömning i samband med införande av bestämmelsen i LEK var att rättsläget därigenom inte förändrades i detta avseende (prop. 2002/03:110 s. 255).

Principen om eterns frihet har under senare år emellertid i viss mån ifrågasatts och det kan inte längre anses självklart var gränsen för principens tillämpning går. Lagrådet har i yttrande den 9 februari 2007 över förslaget till lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, anfört att principen allt mer torde kunna ifrågasättas när en allt större del av vår privata kommunikation blir eterburen. Lagrådet framhöll att bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning (sedan den 1 juli 2012 benämnda hemlig avlyssning av elektronisk kommunikation respektive hemlig övervakning av elektronisk kommunikation) inte gör någon skillnad mellan fast telefoni och mobil trådlös telefoni och att Europadomstolen i sin praxis har ställt samma krav på villkoren för avlyssning av trådlös kommunikation som i fråga om annan telekommunikation. Lagrådet pekade vidare på att det globala nätet är uppbyggt på ett sådant sätt att det kan bero på slumpartade förhållanden om en viss kommunikation förmedlas delvis i tråd, delvis trådlöst (se Lagrådets yttrande i prop. 2006/07:63 s. 170–171, jfr också SOU 2003:32 s. 268–269, 2007:22 del 1 s. 255–256 och 2008:3 s. 261–262).

I sammanhanget bör också nämnas att rättigheten att för försvarsunderrättelseändamål använda signalspaning om signalerna befinner sig i etern, inte längre direkt härleds från principen om eterns frihet. Möjligheten till signalspaning regleras istället i dag i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, oavsett om signalerna befinner sig i etern eller tråd. Sedan den 1 januari 2013 får även Säkerhetspolisen och Rikskriminalpolisen, och inte som tidigare enbart regeringen, Regeringskansliet eller Försvarsmakten, inrikta signalspaning i försvarsunderrättelseverksamhet med stöd av den lagen (jfr också förslagen i SOU 2009:66 om att ta fram ett nytt regelverk för signalspaning, där inhämtningsmetoden tillåts användas för polisen direkt i syfte att såväl förebygga och förhindra som att utreda brott).

För brytande av post- eller telehemlighet döms den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller i ett elektroniskt kommunikationsnät. Med elektroniskt kommunikationsnät avses detsamma som i LEK (se 1 kap. 7 § den lagen). Straffet är böter eller fängelse i högst två år. Bestämmelsen skyddar såväl meddelanden i traditionell form som elektroniska meddelanden och omfattar intrång i den sist nämnda typen av meddelanden oavsett på vilket sätt dessa tekniskt förmedlas. Eftersom straffbestämmelsen förutsätter att någon *olovligen* bereder sig tillgång till meddelandet har emellertid ansetts att den, mot bakgrund av principen om eterns frihet, inte kan tillämpas i fråga om meddelanden som befordras via radio (prop. 1992/93:200 s. 157–158, se även prop. 2006/07:66 s. 41). Olovlighetsrekvisitet anses i ett sådant fall inte uppfyllt. Skyddet sträcker sig från den tidpunkt när meddelandet har avlämnats för befordran till dess att meddelandet har nått mottagaren (Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 4:35). Med post- och telebefordringsföretag avses företag som på affärsmässiga grunder huvudsakligen förmedlar information – meddelanden i form av postförsändelser och olika former av meddelanden i ett elektroniskt kommunikationsnät – som andra lämnar för distribution (prop. 1992/93:200 s. 161–162). I den mån meddelanden i ett elektroniskt kommunikationsnät befordras på annat sätt än via ett telebefordringsföretag, exempelvis via privata kommunikationsnät, skyddas de inte av straffbestämmelsen.

Begreppet ”bereda sig tillgång till” innebär inte att gärningsmannen verkligen fått del av innehållet i meddelandet, utan det är tillräckligt att han eller hon getts möjlighet att få del av det (Berggren

m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 4:36, jfr motsvarande begrepp i dataintrångsbestämmelsen avsnitt 5.3.2 och nedan). För straffansvar förutsätts att gärningen begås med uppsåt att bereda gärningsmannen tillgång till meddelande och straffansvaret träffar alltså inte den som oavsiktligt får tillgång till ett meddelande (Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 4:36).

Försök till brytande av post- eller telehemlighet är inte straffbart. Däremot är förberedelse till brytande av telehemlighet straffbar genom en särskild bestämmelse i 4 kap. 9 b § brottsbalken. Om någon anbringar ett tekniskt hjälpmedel med uppsåt att bryta telehemlighet på sätt som sägs i 4 kap. 8 § brottsbalken ska han dömas för förberedelse till sådant brott, under förutsättning att han inte gjort sig skyldig till fullbordat brott.

Som framgått i avsnitt 5.3.2 straffbeläggs enligt dataintrångsbestämmelsen, vilken är subsidiär till bestämmelsen om brytande av post- eller telehemlighet, bl.a. att olovligen bereda sig tillgång till en *uppgift som är avsedd för automatiserad behandling*. För tillämpningen av begreppet ”uppgift som är avsedd för automatiserad behandling” är det, som nämnts i avsnittet, utan betydelse var uppgifterna finns eller förvaras i systemet, vilket innebär att alla uppgifter, oavsett på vilket datamedium de finns, omfattas. Också uppgifter som är under befordran omfattas därmed, oavsett på vilket sätt befordran sker. Genom att bestämmelsen även tar sikte på uppgifter under befordran är den alltså tillämplig även på avlyssning av datorbehandlingsbara uppgifter. För straffansvar är det, som framgått, tillräckligt att någon *bereder sig tillgång till* en uppgift som är avsedd för automatiserad behandling. Personen behöver inte de facto ta del av uppgifterna, utan det är tillräckligt att personen har fått möjlighet att göra detta. Även i det fall någon avlyssnar elektromagnetisk strålning, som visserligen inte innehåller datorbehandlingsbara uppgifter, men vilken kan omvandlas till sådana uppgifter, torde ansvar för dataintrång därför kunna komma ifråga. Personen har ju genom åtgärden gett sig själv en möjlighet att få del av en sådan uppgift, även om ytterligare en åtgärd behöver vidtas, dvs. att omvandla strålningen till logisk information.

Dataintrångsbestämmelsen förutsätter emellertid för straffansvar att gärningen är olovlig. Som tidigare framgått anses principen om eterns frihet för straffrättens del innebära att bestämmelsen om brytande av telehemlighet i princip inte är tillämplig på intrång i radiobefordrade meddelanden. Det anses följa av att bestämmelsens krav på olovlighet inte är uppfyllt. På samma grund som beträffande

bestämmelsen om brytande av telehemlighet har därför uttalats att inte heller dataintrångsbestämmelsen *som regel* kan anses vara tillämplig på intrång i radiobefordrade uppgifter (prop. 2006/07:66 s. 41). Vad däremot gäller andra angrepp som t.ex. manipulation i form av ändring eller radering av uppgifter som befordras har ansetts att dataintrångsbestämmelsen kan vara tillämplig även på uppgifter som befordras via radio (prop. 2006/07:66 s. 41). Ansvar för dataintrång har även ansetts kunna komma i fråga för intrång i radiobefordrade uppgifter som är krypterade (prop. 2006/07:66 s. 49). Att dataintrångsbestämmelsen på detta sätt omfattar även radiobefordrade uppgifter har alltså inte ansetts vara oförenligt med principen om eterns frihet.

När det gäller bl.a. dataintrångsbestämmelsen och förhållandet till grundlagarna bör följande nämnas. Yttrandefriheten innebär en rätt för var och en att skaffa fram uppgifter i vilket ämne som helst för att lämna dem för publicering eller för att publicera dem själv i grundlagsskyddade medier (1 kap. 1 § tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen). Grundlagarna tillåter emellertid att denna frihet begränsas genom att själva *tillvägagångssättet* regleras (1 kap. 9 § 5 p. tryckfrihetsförordningen och 1 kap. 12 § första stycket yttrandefrihetsgrundlagen). När exempelvis dataintrångsbestämmelsen straffbelägger att olovligen – genom avlyssning eller på annat sätt – bereda sig tillgång till en uppgift som är avsedd för automatiserad behandling, avser det sättet för införskaffande av information. Det finns därför stöd för en sådan kriminalisering i de nämnda grundlagsbestämmelserna, även när anskaffandet sker i syfte att publicera informationen.

Som nämnts måste det i dag anses vara oklart hur långt principen om eterns frihet sträcker sig. Principen har sin grund i uttalanden i förarbeten som gjordes innan utvecklingen på teknikområdet nått så långt som i dag. Det bakomliggande syftet med de uttalanden som då gjordes synes främst ha varit att, i ett allmänt demokratisyfte, garantera medborgarna rätt att ta del av radioutsändningar. I sammanhanget bör artikel 8 i Europakonventionen framhållas. Enligt artikeln har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Denna rättighet får inte inskränkas av det allmänna annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa närmare angivna ändamål. Konventionsbestämmelsen ger enligt Europadomstolens praxis upphov inte bara till en negativ förpliktelse för det allmänna att avhålla sig från omotiverade inskränkningar i denna rättighet

utan även en *positiv skyldighet* för det allmänna att se till att enskilda även i förhållande till andra enskilda tillförsäkras en rätt till skydd för privat- och familjeliv (se prop. 2009/10:80 s. 174 och Danelius, *Mänskliga rättigheter i europeisk praxis, En kommentar till Europakonventionen om de mänskliga rättigheterna*, 2007, s. 302). Ett sådant skydd tillförsäkras bl.a. genom kriminalisering av olika åtgärder som innefattar intrång i den personliga integriteten. Att principen om eterns frihet i dagens läge, när gränsen mellan trådbunden och eterbunden trafik allt mer suddats ut och människor som kommunicerar med varandra inte ens vet på vilket sätt informationsöverföringen sker, skulle innebära en rätt för envar att avlyssna vilken trafik som helst, så länge som den är eterburen, är svårt att förena med artikel 8 i Europakonventionen.

Av det som tidigare anförts framgår att det som konventionen betecknar som olaglig avlyssning kan vara straffbart som brytande av telehemlighet, om det är fråga om överföring av meddelanden via ett allmänt kommunikationsnät, med viss reservation för meddelanden som befordras via radio. I övrigt kan det vara straffbart som dataintrång, även här med viss reservation för avlyssning av överföring som ägt rum genom radiovågor.

När det gäller avlyssning av elektromagnetiska signaler behöver sådan avlyssning, som enligt konventionen ska vara straffbelagd, inte ha ägt rum vid befordran av uppgifter, utan genom avlyssning av sådan strålning som sänts ut av en dator som varit påslagen. Det innebär att det inte omfattas av brottet brytande av telehemlighet. Som tidigare anförts kan emellertid avlyssning av sådan strålning, som i och för sig inte innehåller några datorbehandlingsbara uppgifter, anses innebära att någon berett sig tillgång till uppgifter avsedda för automatiserad behandling, eftersom signalerna kan omvandlas till sådana uppgifter. Även ett sådant förfarande kan således vara straffbart som dataintrång. Det som konventionsartikeln avser att kriminalisera när det gäller avlyssning av elektromagnetiska emissioner, synes ta sikte på sådan ”oavsiktlig” strålning som kan sändas ut av en dator under drift. Avlyssning av sådan strålning, även om den består av radiovågor, kan inte anses speciellt skyddsvärd inom ramen för principen om eterns frihet. Principen tar, som nämnts, närmast sikte på möjligheten att kunna ta emot radioprogram, medan det bakomliggande syftet med avlyssning av elektromagnetisk strålning (om avlyssningen inte sker oavsiktligt) är att ur den få fram uppgifter. För att få fram logisk information ur strålningen torde krävas speciella tekniska hjälpmedel, dvs. inte enbart en vanlig

radioapparat. Det kan mot den angivna bakgrunden ifrågasättas om principen om eterns frihet alls inbegriper den typ av avlyssning av elektromagnetiska signaler som nu avses.

Konventionsartikeln straffbelägger, som framgått, enbart att *orättmätigt* avlyssna icke allmänna överföringar av datorbehandlingsbara uppgifter. Syftet med artikeln är inte heller, som nämnts, att avlyssning av varje radioöverföring som inte är allmän ska kriminaliseras. Begreppet orättmätigt får sitt innehåll av det sammanhang det används i, och det står varje fördragsslutande stat fritt att tolka begreppet utifrån sin nationella rätt. Ett handlande som är tillåtet i enlighet med etablerade principer i ett land begås således inte orättmätigt (se den förklarande rapporten p. 38). Utifrån detta resonemang kan således hävdas att svensk rätt genom bestämmelserna om brytande av post- eller telehemlighet och dataintrång, av vilka den senare redan kriminaliserar de viktigaste formerna av avlyssning av datorbehandlingsbara uppgifter, däribland bl.a. intrång i radiobefordrade krypterade uppgifter, uppfyller kraven i konventionen på kriminalisering av olovlig avlyssning. Som vi tidigare anfört bör vidare principen om eterns frihet inte anses omfatta sådan avlyssning av elektromagnetiska emissioner som konventionen avser att straffbelägga, varför svensk rätt i denna del genom dataintrångsbestämmelsen redan uppfyller konventionens krav.

I sammanhanget kan återknytas till vad som i avsnitt 5.3.2 sagts om den norska motsvarigheten till dataintrångbestämmelsen. Som framgått döms i Norge den för dataintrång som genom att bryta en säkerhetsåtgärd eller på liknande sätt oberättigat bereder sig tillgång till uppgifter eller program som är lagrade eller som överförs med elektroniska eller tekniska hjälpmedel (straffeloven § 145 andra stycket). Bestämmelsen anses även tillämplig på olika former av avlyssning av datorbehandlingsbara uppgifter och även på avlyssning av elektromagnetisk strålning, om strålningen kan omskapas till logisk information (se Datakrimutvalgets betänkande *Lovtiltak mot datakriminalitet*, NOU 2003:27, s.16). Mot den bakgrunden ansågs bestämmelsen uppfylla kraven på kriminalisering i artikel 3 och något behov av lagändringar för att kunna tillträda konventionen ansågs inte föreligga med anledning av artikeln (se den norska propositionen Ot.prp. nr. 40, [2004–2005] s. 12). Det bör i sammanhanget nämnas att principen om eterns frihet anses vara inte bara en svensk utan en vedertagen internationell princip.

Sammanfattningsvis är det vår uppfattning att svensk rätt, mot bakgrund av de överväganden som gjorts ovan om dels räckvidden

av principen om eterns frihet, dels begreppet ”orättmätigt”, genom bestämmelsen om brytande av post- eller telehemlighet och dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som olaglig avlyssning. Krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem behöver enligt vår mening inte uppställas vid ett tillträde till konventionen.

Här bör nämnas att i det förslag till EU-direktiv som avses ersätta rambeslutet upptas en bestämmelse om olaglig avlyssning (artikel 6) som i princip överensstämmer med konventionens artikel 3 (se närmare avsnitt 7.3.4). I förslaget anges att med begreppet *orättmätigt* i de olika artiklarna i direktivet avses ”intrång eller störning som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta eller som inte medges i den nationella lagstiftningen” (artikel 2 d).

5.3.5 Datastörning (artikel 4)

Bedömning: Svensk rätt uppfyller genom främst dataintrångsbestämmelsen konventionens krav på vilka handlingar som ska vara straffbelagda som datastörning. Möjligheten att förbehålla sig rätten att uppställa krav på att handlandet som innebär datastörning medför allvarlig skada behöver inte utnyttjas.

Skälen för bedömningen

Enligt *artikel 4* ska det vara straffbart som datastörning att uppsåtligen orättmätigt skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter. Krav får uppställas på att handlandet medför allvarlig skada.

Enligt den förklarande rapporten (p. 60) är syftet med bestämmelsen att åstadkomma skydd för datorbehandlingsbara uppgifter och datorprogram mot uppsåtlig skadegörelse, motsvarande det som finns för materiella ting. Handlingarna som räknas upp i artikeln är avsiktligt delvis överlappande (se den förklarande rapporten p. 61).

Artikeln förutsätter att gärningen begås med *uppsåt* och att den utförs *orättmätigt*. Kravet på att handlingen ska vara orättmätig innebär att exempelvis handlingar som vidtas med samtycke av den som

innehar uppgifterna inte omfattas (se den förklarande rapporten p. 62).

Som framgått i avsnitt 5.3.2 straffbelägger den svenska dataintrångsbestämmelsen att olovligen *ändra* eller *utplåna* en uppgift som är avsedd för automatiserad behandling. Dessa förfaranden måste anses motsvara de åtgärder i artikel 4 som benämns *skada*, *radera*, *försämra* eller *ändra* (jfr bedömningen av motsvarande bestämmelse i EU:s rambeslut om angrepp mot informationssystem, prop. 2006/07:66 s. 28). Som nämnts i avsnitt 5.3.4 måste begreppet *uppgift som är avsedd för automatiserad behandling* i dataintrångsbestämmelsen vidare anses motsvara vad som enligt konventionen ska förstås med *datorbehandlingsbara uppgifter*.

Enligt artikeln ska det vidare vara straffbelagt att orättmätigt *undertrycka* datorbehandlingsbara uppgifter. Av den förklarande rapporten (p. 61) framgår att med uttrycket avses en handling som hindrar eller avbryter åtkomsten till uppgiften för den person som har tillgång till datorn eller datamediet som uppgiften är lagrad på. Att på detta sätt undertrycka en uppgift torde många gånger samtidigt innebära att uppgifter enligt dataintrångsbestämmelsen ändras eller utplånas. Sedan 2007 är det dock, som framgått i avsnitt 5.3.2, även straffbart enligt dataintrångsbestämmelsen att olovligen *blockera* en uppgift som är avsedd för automatiserad behandling. Med ”blockera” avses just hindrande eller spärrande åtgärder av olika slag (prop. 2006/07:66 s. 50). Därmed träffas sådana förfaranden som i konventionen avses med att undertrycka uppgifter.

Såväl dataintrångsbestämmelsen som artikel 4 förutsätter att gärningen begås med *uppsåt*. Begreppet *orättmätigt* i artikel 4 får anses motsvara begreppet *olovligen* i dataintrångsbestämmelsen (jfr bedömningen i avsnitt 5.3.3).

De förfaranden som beskrivs i konventionens artikel 4 kan i svensk rätt i vissa fall även tänkas motsvara andra brott, främst *skadegörelse* och *sabotage*.

Att förstöra eller skada egendom, fast eller lös, till men för annans rätt därtill, är straffbart som *skadegörelse* (12 kap. 1 § brottsbalken). Straffet är böter eller fängelse i högst ett år. Om gärningen har inneburit synnerlig fara för någons liv eller hälsa eller skadan drabbat sak av stor kulturell eller ekonomisk betydelse eller skadan annars är synnerligen kännbar, är gärningen att anse som *grov skadegörelse* (12 kap. 3 § brottsbalken). Straffet är fängelse i högst fyra år.

För *sabotage* döms den som förstör eller skadar egendom, som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskip-

ning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet i riket, eller genom annan åtgärd, som inte innefattar endast undanhållande av arbetskraft eller uppmaning därtill, allvarligt stör eller hindrar användningen av sådan egendom (13 kap. 4 § brottsbalken). Detsamma gäller om någon annars genom skadegörelse eller annan åtgärd som nyss sagts allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel eller av anläggning för allmänhetens förseende med vatten, ljus, värme eller kraft. Straffet är fängelse i högst fyra år. Om fara för rikets säkerhet, för flera människoliv eller för egendom av särskild betydelse framkallats genom brottet, döms för *grovt sabotage* (13 kap. 5 § brottsbalken). Straffet är fängelse på viss tid, lägst två och högst arton år, eller på livstid. Grov skadegörelse, sabotage och grovt sabotage är dessutom straffbart som *terroristbrott* enligt lagen (2003:148) om straff för terroristbrott under de förutsättningar som anges i den lagen.

Såväl skadegörelse- som sabotagebestämmelserna avser angrepp på egendom som medför att egendomen förstörs eller skadas. Normalt förutsätts att saken verkligen undergår en förändring och att skadan inte är av endast tillfällig natur (jfr Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 12:3). Sabotagebrottet omfattar dessutom andra åtgärder som allvarligt stör eller hindrar användningen av viss egendom.

Dessa straffbestämmelser kan således omfatta vissa av de situationer som ska vara straffbara enligt artikel 4 som datastörning. De torde t.ex. kunna tillämpas i vissa fall när handlandet *samtidigt* innebär att datorer eller program skadas. Om sådana uppgifter som avses i bestämmelsen om dataintrång även skadas blir emellertid också denna bestämmelse tillämplig. Eftersom brottet dataintrång har en strängare straffskala än skadegörelse av normalgraden konsumeras dock vanligtvis skadegörelsebrottet. Skulle gärningen emellertid orsaka allvarlig fysisk skada kan ansvar för grov skadegörelse dömas ut i konkurrens med dataintrånget (Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 12:4). I sammanhanget bör vidare anmärkas att sabotagebestämmelsen, till skillnad från konventionsartikeln, tar sikte på viss för samhället särskilt viktig egendom.

Sammanfattningsvis gör vi bedömningen att svensk rätt genom främst dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som datastörning. Någon anledning att utnyttja möjligheten att förbehålla sig rätten att uppställa krav

på att handlandet som avses i artikeln medför allvarlig skada finns inte.

I sammanhanget bör nämnas att konventionens artikel 4 i huvudsak motsvarar artikel 4 i EU:s rambeslut om angrepp mot informationssystem. Vid genomförandet av rambeslutet i svensk rätt straffbelades som dataintrång bl.a. att blockera en uppgift som är avsedd för automatiserad behandling. Genom denna ändring av dataintrångsbestämmelsen ansågs svensk rätt uppfylla den aktuella artikeln i rambeslutet (prop. 2006/07:66 s. 27–28 och 42–43). Vidare bör nämnas att i det förslag till direktiv som avses ersätta rambeslutet upptas en bestämmelse om olaglig datastörning (artikel 5) som i princip överensstämmer med artikel 4 i rambeslutet, och därmed också med konventionens artikel 4 (se närmare avsnitt 7.3.3).

Här kan också nämnas att i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att om de ändringar i dataintrångsbestämmelsen som vid tiden för promemorian föreslagits (i promemorian *Angrepp mot informationssystem*, Ds 2005:5) som ett led i genomförandet av EU:s rambeslut om angrepp mot informationssystem genomfördes, uppfyllde svensk rätt, genom dataintrångsbestämmelsen, kraven på kriminalisering i konventionens artikel 4 (Ds 2005:6, s. 212–215).

5.3.6 Systemstörning (artikel 5)

Bedömning: Svensk rätt uppfyller genom främst dataintrångsbestämmelsen konventionens krav på vilka handlingar som ska vara straffbelagda som systemstörning.

Skälen för bedömningen

Enligt *artikel 5* ska det vara straffbart som systemstörning att uppsåtligen orättmätigt allvarligt hindra ett datorsystems drift genom att mata in, överföra, skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

Enligt den förklarande rapporten (p. 65) är syftet med bestämmelsen att säkerställa att datorsystem kan fungera utan störningar.

Den handling som ska vara straffbelagd består alltså i att allvarligt hindra ett datorsystems drift. Angående definitionen av begreppet datorsystem, se avsnitt 5.2. Hur störningen av driften kan åstad-

kommas anges, som framgått, genom en uppräkning av olika åtgärder med datorbehandlingsbara uppgifter. Angående definitionen av begreppet datorbehandlingsbara uppgifter, se avsnitt 5.2.

De åtgärder som kan vidtas är dels sådana som riktar sig mot befintliga datorbehandlingsbara uppgifter i ett datorsystem, dvs. att skada, radera, försämra, ändra eller undertrycka uppgifter, dels sådana som innebär att datorbehandlingsbara uppgifter matas in eller överförs. De uppräknade åtgärderna som riktar sig mot befintliga datorbehandlingsbara uppgifter motsvarar de åtgärder som räknas upp i artikel 4 som åtgärder som, i vid mening, skadar datorbehandlingsbara uppgifter och som således ska straffbeläggas som datastörning. Vad avser förfaranden som innebär att datorbehandlingsbara uppgifter matas in eller överförs behöver de inte innebära att de befintliga uppgifterna i systemet skadas. Det kan exempelvis vara fråga om s.k. överbelastningsattacker, vid vilka så stora mängder e-post sänds att mottagarens system överbelastas eller blockeras (se den förklarande rapporten p. 69). Attacken riktar sig då således inte mot de datorbehandlingsbara uppgifterna i systemet utan mot själva systemet och dess funktion.

Som framgått, ska handlandet innebära att ett datorsystems drift *allvarligt* hindras. Det är en uppgift för varje fördragsslutande stat att själv fastställa vilka kriterier som ska vara uppfyllda för att driften ska anses ha allvarligt hindrats (se den förklarande rapporten p. 67).

Artikeln förutsätter att gärningen begås med *uppsåt* och att den utförs *orättmätigt*. Som nämnts i avsnitt 5.3.3 innebär kravet på att handlingen ska vara orättmätig att handlingar som vidtas med samtycke av den som innehar uppgifterna, exempelvis för att testa systemets säkerhet, inte omfattas (se den förklarande rapporten p. 68).

Som framgått i avsnitt 5.3.2 kriminaliserar den svenska dataintrångsbestämmelsen inte direkt ett allvarligt hindrande av driften av ett datorsystem. Däremot straffbeläggs vissa förfaranden med uppgifter som är avsedda för automatiserad behandling. I den utsträckning dessa motsvarar de åtgärder som räknas upp i artikel 5, måste dataintrångsbestämmelsen anses uppfylla det krav på kriminalisering som artikeln innebär, eftersom bestämmelsen straffbelägger åtgärderna i sig utan krav på att driften av datorsystemet påverkas (jfr motsvarande bedömning när det gäller artikeln om olaglig systemstörning i EU:s rambeslut om angrepp mot informationssystem, prop. 2006/07:66 s. 25).

Systemstörningen ska bl.a. bestå i att *skada*, *radera*, *försämra* eller *ändra* datorbehandlingsbara uppgifter. Som angetts i avsnitt 5.3.5

måste dessa handlingar anses motsvara vad som enligt dataintrångsbestämmelsen är straffbelagt som att *ändra* eller *utplåna* en uppgift som är avsedd för automatiserad behandling (jfr bedömningen av motsvarande bestämmelse i EU:s rambeslut om angrepp mot informationssystem, prop. 2006/07:66 s. 26). Vad gäller de övriga åtgärder som anges i artikeln, dvs. att *mata in*, *överföra* eller *undertrycka* datorbehandlingsbara uppgifter kan dessa i många fall samtidigt tänkas innebära att uppgifter enligt dataintrångsbestämmelsen ändras eller utplånas. Det är vidare också, som angetts i avsnitt 5.3.2, straffbart enligt dataintrångsbestämmelsen att föra in en uppgift i register.

Som angetts i tidigare avsnitt är det dock sedan 2007 även straffbart enligt dataintrångsbestämmelsen att olovligen *blockera* en uppgift som är avsedd för automatiserad behandling, vilket innebär att sådana förfaranden som i konventionen avses med att *undertrycka* uppgifter i huvudsak träffas.

Trots att dataintrångsbestämmelsen omfattar även den som blockerar en uppgift avsedd för automatiserad behandling straffbeläggs inte genom tillägget om blockering exempelvis inmatning av virusprogram eller överföring av en stor mängd automatiskt genererade meddelanden som kraftigt påverkar driften av ett system och därmed också användningen av de uppgifter som finns i systemet utan att uppgifterna helt blockeras (prop. 2006/07:66 s. 44). Som framgått i avsnitt 5.3.2 omfattar dataintrångsbestämmelsen sedan 2007 dock även den som olovligen genom någon annan liknande åtgärd än de som redovisats ovan *allvarligt stör eller hindrar användningen av* en uppgift som är avsedd för automatiserad behandling. Det straffbara förfarandet tar, som angetts, sikte på åtgärder som verkar på ett sådant sätt att de stör eller hindrar att uppgifter som är avsedda för automatiserad behandling kan användas på avsett sätt, dvs. åtgärder som påverkar driften av ett system och därmed också användningen av de uppgifter som finns i systemet utan att uppgifterna helt blockeras, t.ex. i form av tillgänglighetsattacker eller överbelastningsattacker (prop. 2006/07:66 s. 43–44 och 50).

Såväl dataintrångsbestämmelsen som artikel 5 förutsätter att gärningen begås med *uppsåt*. Begreppet *orättmätigt* i artikel 5 får anses motsvara begreppet *olovligen* i dataintrångsbestämmelsen (jfr bedömningen i avsnitt 5.3.3).

Sammanfattningsvis är vår bedömning att svensk rätt genom främst dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som systemstörning.

I sammanhanget bör nämnas att konventionens artikel 5 i huvudsak motsvarar artikel 3 i EU:s rambeslut om angrepp mot informationssystem. Vid genomförandet av rambeslutet i svensk rätt straffbelades, som framgått av avsnitt 5.3.2, som dataintrång bl.a. att blockera en uppgift som är avsedd för automatiserad behandling. Vidare utvidgades dataintrångsbestämmelsen till att omfatta även den som olovligen, genom någon annan liknande åtgärd än de som uttryckligen räknas upp i bestämmelsen, allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling. Genom ändringarna av dataintrångsbestämmelsen ansågs svensk rätt uppfylla den aktuella artikeln i rambeslutet (prop. 2006/07:66 s. 25–27 och 43–45). Vidare bör nämnas att i det förslag till direktiv som avses ersätta rambeslutet upptas en bestämmelse om olaglig systemstörning (artikel 4) som i princip överensstämmer med artikel 3 i rambeslutet, och därmed också med konventionens artikel 5 (se närmare avsnitt 7.3.2).

Här kan också nämnas att i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att om de ändringar i dataintrångsbestämmelsen som vid tiden för promemorian föreslagits (i promemorian *Angrepp mot informationssystem*, Ds 2005:5) som ett led i genomförandet av EU:s rambeslut om angrepp mot informationssystem genomfördes, uppfyllde svensk rätt, genom dataintrångsbestämmelsen, kraven på kriminalisering i konventionens artikel 5 (Ds 2005:6, s. 212–215).

5.3.7 Missbruk av apparatur (artikel 6)

Bedömning: Svensk rätt uppfyller genom bestämmelserna om förberedelse till brott konventionens krav på vad som ska vara straffbelagt som missbruk av apparatur.

Skälen för bedömningen

Enligt *artikel 6* ska viss *befattning* (att tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra) med olika typer av *verktyg* (apparat vari ingår ett datorprogram som är skapat eller anpassat främst för att begå något av brotten enligt artiklarna 2–5, samt datorlösenord, åtkomstkod eller liknande datorbehandlingsbara uppgifter som kan ge åtkomst till ett helt dator-

system eller del därav) utgöra ett brott, om gärningen är uppsåtlig och utförs orättmätigt i syfte (dvs. med direkt uppsåt) att brott enligt artiklarna 2–5 ska begås. Även att inneha något sådant som nämnts med uppsåt att det ska användas för att begå något av brotten enligt artiklarna 2–5 ska straffbeläggas. Krav får emellertid därvid uppställas på att flera sådana föremål ska innehas för att straffansvar ska gälla.

I förtydligande syfte anges särskilt att artikeln inte ska tolkas så att den kräver straffansvar i de fall där tillverkning, försäljning, anskaffning för användning, import, spridning eller annat tillgängliggörande eller innehav som avses i artikeln inte har till syfte att något av brotten enligt artiklarna 2–5 ska begås, såsom exempelvis för att i behörig ordning testa eller skydda ett datorsystem (se artikel 6.2).

En fördragsslutande stat får förbehålla sig en möjlighet att inte straffbelägga vissa av de gärningar som räknas upp i artikeln, om förbehållet inte avser försäljning, spridning eller annat tillgängliggörande av datorlösenord, åtkomstkod eller liknande datorbehandlingsbara uppgifter som kan ge åtkomst till datorsystem (artikel 6.3 och 42).

Enligt den förklarande rapporten (p. 71) är syftet med bestämmelsen att åstadkomma en möjlighet att effektivt bekämpa brotten i artiklarna 2–5 redan innan de hunnit begås. Brotten i de nämnda artiklarna kräver, enligt rapporten, ofta tillgång till olika former av verktyg för åtkomst (”hacker-verktyg”) eller andra verktyg, vilket innebär att det finns incitament att få tillgång till dem, i syfte att begå brott. Detta leder i sin tur till att det finns en risk för att det skapas en svart marknad för sådana verktyg, vilket, i brottsbekämpande syfte, bör förhindras.

Artikeln omfattar alltså inte enbart sådan apparatur som *uteslutande* skapats i syfte att begå brott, eftersom detta skulle leda till ett för snävt tillämpningsområde och helt utesluta apparatur med dubbla användningsområden, dvs. som kan användas både i legitima och illegitima syften. I stället omfattar artikeln apparatur som objektivt sätt *primärt* är tänkt att användas för att begå brott, vilket i de flesta fall kommer att utesluta apparatur som även har ett legalt användningsområde (se den förklarande rapporten p. 73).

Som framgått förutsätter artikeln att gärningen begås inte bara uppsåtligen utan med *direkt uppsåt* att hjälpmedlet (datorprogrammet, datorlösenordet etc.) ska användas för att begå något av brotten i artiklarna 2–5 (se den förklarande rapporten p. 76).

Att utan lov ta befattning med apparatur eller verktyg på det sätt som beskrivs i artikeln kan enligt svensk rätt utgöra *förberedelse till brott*.

Som vi redogjort för i avsnitt 5.3.3–5.3.6 uppfyller svensk rätt främst genom bestämmelsen om dataintrång konventionens krav på kriminalisering av brotten i artiklarna 2–5, samtidigt som vissa av brotten i svensk rätt även kan motsvara brytande av telehemlighet, skadegörelse och sabotage. Förberedelse till dataintrång är straffbart, om det fullbordade brottet inte skulle ha varit att anse som ringa (4 kap. 10 § brottsbalken). Som framgått i avsnitt 5.3.1 tillåter konventionen generellt att ringa brott undantas från kriminalisering (se den förklarande rapporten p. 37). Även förberedelse till grov skadegörelse, sabotage och grovt sabotage är straffbart (12 kap. 5 § resp. 13 kap. 12 § brottsbalken). Som nämnts i avsnitt 5.3.4 är förberedelse till brytande av telehemlighet genom visst angivet förfarande straffbelagt i en särskild bestämmelse i brottsbalken (4 kap. 9 b §).

Enligt 23 kap. 2 § brottsbalken ska 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.

För att någon ska kunna dömas för ett förberedelsebrott krävs att det förelegat fara för att brottet skulle ha fullbordats och att denna fara inte var ringa. Dessutom krävs det att det särskilt har föreskrivits att förberedelse till den aktuella brottstypen är straffbar. Ansvar för förberedelse till brott förutsätter också, på ett mer allmänt plan, att händelseförloppet inte fortlöpt så långt att ansvar för fullbordat brott eller försök till brott kan utdömas. Det krävs också att det är fråga om förberedelse till ett uppsåtligt brott. Förberedelse till oaktsamhetsbrott, i den mån sådan alls kan förekomma, är inte straffbart (jfr prop. 2000/01:85 s. 32). Gärningsmannens uppsåt behöver inte avse en viss bestämd gärning utan det räcker att uppsåtet avser att brott av visst slag förr eller senare kommer till stånd (Berggren m.fl., *Brottsbalken En kommentar Kap. 13–24*, s. 23:28).

Straffet för förberedelse ska bestämmas under den högsta och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre

straff än fängelse i två år får bestämmas endast om fängelse i åtta år eller däröver kan följa på det fullbordade brottet.

Straffansvaret för förberedelse till brott reformerades och utvidgades i viss mån den 1 juli 2001. Begreppet hjälpmedel i paragrafen ändrades således genom att den tidigare normerande uppräkningen som fanns i bestämmelsen slopades och ersattes av det mer generella rekvisitet: ”något som är särskilt ägnat att användas som hjälpmedel vid ett brott”. Det reformerade hjälpmedelsbegreppet avses omfatta dels sådana föremål som knappast har något annat användningsområde än att begå brott med (exempelvis ett avsågat hagelgevär), dels sådana föremål som också kan ha ett legalt användningsområde, t.ex. vapen eller olika former av brytverktyg att användas vid inbrott (prop. 2000/01:85 s. 50). De objekt som faller under bestämmelserna kan vara av vilket slag som helst och således kan inte bara befattning med fysiska föremål utan även immateriella objekt vara straffbar som förberedelse. Såsom särskilt ägnat att användas som hjälpmedel vid brottet bör således, enligt motiven, bl.a. datavirus räknas, liksom annan programvara som är framställd t.ex. uteslutande i syfte att begå dataintrång eller andra typer av brott, exempelvis olika former av förfalskning (prop. 2000/01:85 s. 41 och 50).

Begreppet hjälpmedel avser enligt motiven också t.ex. *samlingar av information*, såsom en sammanställning av ett antal koder till olika datorsystem, som nedtecknats i syfte att användas vid dataintrång (prop. 2000/01:85 s. 50).

För att ett hjälpmedel ska anses vara särskilt ägnat att användas som hjälpmedel vid brott, bör, enligt motiven, allmänt sett krävas att det med hänsyn till sin beskaffenhet är av någorlunda *central betydelse* för brottets genomförande (prop. 2000/01:85 s. 41). Kvalificeringen av hjälpmedlet ska således göras genom en objektiv bedömning och hjälpmedlet ska vara *typiskt sett lämpat* för det aktuella brottet. Förutom rena brottsverktyg anses därför, som nämnts, bl.a. sammanställd information om objektet för brottet omfattas, dock förutsatt att informationen är nedtecknad eller annars lagrad på ett sådant sätt att den kan sägas utgöra hjälpmedel (prop. 2000/01:85 s. 41).

När det gäller det verktyg som först räknas upp i artikel 6 (*en apparat vari ingår ett datorprogram som är skapat eller anpassat främst för att begå något av brotten enligt artiklarna 2–5*; se artikel 6.1 a i) omfattas de, sedan 2001, av hjälpmedelsbegreppet i förberedelsebestämmelsen. Även övriga verktyg som nämns i artikeln (*ett dator-*

lösenord, en åtkomstkod eller liknande datorbehandlingsbara uppgifter; se artikel 6.1 a ii) borde kunna betraktas som något som, i orätta händer, är särskilt ägnat att användas som ett hjälpmedel vid brott. Sådana uppgifter är till för att skydda it-miljöer mot obehöriga och tillgång till dem är ofta en grundläggande förutsättning för intrång i informationssystem. De är således inte sällan av central betydelse för olika former av intrång (jfr det senast refererade motivuttalandet). Förberedelsebestämmelsen får därför anses omfatta att utan lov ta befattning med lösenord, åtkomstkoder och andra liknande uppgifter.

Vad avser de befattningar med verktyg som ska vara kriminaliserade enligt artikel 6.1 a (att *tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra*) måste de fullt ut anses motsvara de förfaranden som är straffbelagda enligt förberedelsebestämmelsen (att *skaffa, tillverka, lämna, ta emot, förvara, transportera, sammanställa eller ta annan liknande befattning*).

Som nämnts, föreskriver artikeln emellertid att det även ska vara straffbart att *inneha* något som räknas upp i artikeln, med uppsåt att det ska användas för att begå något av brotten i artiklarna 2–5. Som förberedelsehandling i 23 kap. 2 § brottsbalken räknas inte särskilt upp att *inneha* ett hjälpmedel. Att inneha något kan karaktäriseras som en *passiv* handling, medan de handlingar som räknas upp i förberedelsebestämmelsen främst är *aktiva*. Uppräkningen i bestämmelsen i 23 kap. 2 § brottsbalken är emellertid så omfattande att det kan förutsättas att alla tänkbara former av innehav träffas av bestämmelsen, exempelvis genom att innehavet föregåtts av ett anskaffande eller tillverkande, eller genom att innehavet vore att anse som ett förvar av hjälpmedlet. Den möjlighet att avge förbehåll när det gäller kriminalisering av att enbart inneha hjälpmedlen som i och för sig står till buds enligt artikelns p. 3 (jfr artikel 42) behöver därför, enligt vår mening, inte utnyttjas.

Sammanfattningsvis gör vi således bedömningen att svensk rätt genom bestämmelserna om förberedelse till brott uppfyller konventionens krav på vad som ska vara straffbart som missbruk av apparatur. Att på olika sätt tillgängliggöra de olika hjälpmedel som avses i konventionsbestämmelsen i syfte att begå något av brotten i artiklarna 2–5 skulle också enligt svensk rätt kunna innefatta medverkan till brotten (23 kap. 4 § brottsbalken). Även medverkan till förberedelse är straffbart.

I sammanhanget bör nämnas att motsvarande bedömning av svensk rätts förenlighet med konventionsartikeln om missbruk av

apparatur gjordes i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6 s. 118–119).

Det bör här vidare nämnas att i det förslag till direktiv som avses ersätta EU:s rambeslut om angrepp mot informationssystem upptas också en bestämmelse som behandlar missbruk av olika typer av verktyg (artikel 7) och som i princip överensstämmer med konventionens artikel 6 (se närmare avsnitt 7.3.5). Förslaget innehåller emellertid inte något krav på att kriminalisera redan innehav av verktyg.

5.3.8 Datorrelaterad förfalskning (artikel 7)

Bedömning: Svensk rätt uppfyller för närvarande inte konventionens krav på vad som ska vara straffbelagt som datorrelaterad förfalskning. Om regeringens förslag till nytt urkundsbegrepp i 14 kap. 1 § brottsbalken antas av riksdagen kommer svensk rätt emellertid genom bestämmelsen om urkundsförfalskning att uppfylla konventionskravet i denna del. Möjligheten att kräva ytterligare rekvisit i form av krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar ska gälla, behöver då inte utnyttjas.

Skälen för bedömningen

Enligt *artikel 7* ska som datorrelaterad förfalskning straffbeläggas uppsåtliga och orättmätiga gärningar som består i att någon matar in, ändrar, raderar eller undertrycker datorbehandlingsbara uppgifter så att icke autentiska uppgifter uppstår. För straffansvar ska det krävas att förfarandet skett med uppsåt att uppgifterna ska beaktas eller ligga till grund för handlande i rättsliga hänseenden som om de vore autentiska, oavsett om uppgifterna är direkt läsbara eller begripliga. Krav får uppställas på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar ska gälla.

Syftet med bestämmelsen är att införa en motsvarighet i elektronisk miljö till det straffansvar som finns för förfalskning av traditionella fysiska handlingar. Det skyddsvärda intresset är således tillförlitligheten i sådana elektroniska uppgifter som har betydelse i rättsliga sammanhang (se den förklarande rapporten p. 81).

Förfalskning kriminaliseras på olika sätt i skilda nationella rättsordningar. I vissa rättsordningar tar straffbestämmelserna sin utgångspunkt i att dokumentets *utställare* är den han eller hon utger sig för att vara, i andra tas sanningshalten i *uppgifterna* som dokumentet innehåller som utgångspunkt. Konventionsartikeln ska förstås så att villfarelsen i fråga om autenticitet i vart fall måste avse utställaren, dvs. den som uppgifterna påstås härröra från, oavsett om innehållet är sant eller inte. Det står emellertid en fördragsslutande stat fritt att gå längre och i begreppet ”autentisk” även innefatta riktigheten i själva uppgifterna (se den förklarande rapporten p. 82).

I svensk rätt straffbeläggs *urkundsförfalskning* i 14 kap. 1 § brottsbalken. Brottet består i att producera en urkund som är falsk (oäkta) och därigenom omedelbart framkalla fara i bevishänseende. Förfalskningsåtgärden kan, som framgår av bestämmelsen, genomföras på flera olika sätt. Straffet för urkundsförfalskning är fängelse i högst två år. I 14 kap. 2 och 3 §§ brottsbalken finns bestämmelser för ringa respektive grova fall av urkundsförfalskning. Straffet för grov urkundsförfalskning är fängelse lägst sex månader och högst sex år och för ringa brott (förvanskning av urkund) böter eller fängelse högst sex månader. Försök och förberedelse till urkundsförfalskning och grov urkundsförfalskning är straffbart (14 kap. 12 § brottsbalken). Detta gäller dock inte om brottet, om det hade fullbordats, skulle ha varit att anse som ringa. Enligt 14 kap. 4 § brottsbalken kan det vara straffbart som undertryckande av urkund att t.ex. förstöra eller undanskaffa en urkund. I 14 kap. 9 § brottsbalken kriminaliseras brukande av något som förfalskats enligt bl.a. 14 kap. 1–3 §§.

Straffansvaret i de nu redovisade bestämmelserna är konstruerat för *konkreta* angreppsobjekt – *urkunder*. I 14 kap. 1 § andra stycket brottsbalken lämnas en exemplifierande uppräkning på handlingar som kan vara urkunder och därmed förfalskningsföremål. Där nämns bl.a. protokoll, kontrakt och skuldebrev. Varje sådan handling betraktas dock inte som urkund, utan det krävs enligt bestämmelsen att handlingen har upprättats till *bevis* eller på annat sätt kan vara av *betydelse som bevis* genom sitt innehåll. I detta ligger att handlingen självständigt ska förmedla ett *föreställningsinnehåll* av visst slag – tankar, fakta eller annat. Av handlingen ska också direkt eller indirekt kunna utläsas en *utställare*. Det ska alltså vara möjligt att identifiera vem som står bakom innehållet i en handling. Vidare ska handlingen ha *originalkaraktär* (se SOU 2007:92 s. 92).

I praxis har vissa av de redovisade bestämmelserna i 14 kap. brottsbalken tillämpats på företeelser som var okända när straffbestäm-

melserna kom till år 1948. Det kan emellertid ifrågasattas i vilken uträckning handlingar i elektronisk miljö har urkundsstatus i den mening som avses i brottsbalken. I sammanhanget bör erinras om det i 1 kap. 1 § brottsbalken intagna förbudet mot analogisk tillämpning av brottsbalkens straffbud.

Elektroniska handlingar som upprättats som bevismedel eller på annat sätt är av betydelse som bevis kan ofta anses uppfylla kraven på *föreställningsinnehåll* och *utställarangivelse* men kravet på att en handling ska ha *originalkaraktär* vållar inte sällan problem i dessa sammanhang. I elektronisk miljö bygger all informationsbehandling på kopiering av digitala data och nya exemplar blir därför identiska med sina förlagor. Om t.ex. en elektroniskt underskriven handling kopieras så att alla data tas med utan ändringar kan alltså flera ”original” uppstå, och kopiering sker ofta eftersom ett elektroniskt original inte är knutet till en unik fysisk bärare så som ett pappersark är knutet till text och underskrift. Elektroniska underskrifter och andra liknande skydd för äkthet knyts i stället till data som representerar handlingen så att varje nytt exemplar håller samma kvalitet. Skillnaden mellan original i elektronisk miljö respektive pappersmiljö kan därför beskrivas så att det i elektronisk miljö kan finnas ett original*innehåll* men inte något original*exemplar* (se SOU 2007:92 s. 110).

Det får sägas råda osäkerhet om i vilken utsträckning elektroniska handlingar för närvarande är att betrakta som urkunder.[5]

I promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att gällande svensk rätt inte uppfyller konventionens krav på kriminalisering av datorrelaterad förfalskning (Ds 2005:6 s. 103–106). Det konstaterades därvid att en handling i elektronisk form i de flesta fall saknar en utställare av det slag som krävs för ansvar enligt 14 kap. brottsbalken och att förfalskning av elektroniska handlingar därför normalt faller utanför straffansvaret för urkundsförfalskning. Vidare konstaterades att det även kan finnas andra brister i grundläggande kriterier, exempelvis i krav på varaktig-

[5] Jfr NJA 2009 s. 111 där frågan var om ett förfarande som bestod i att tillverka förfalskade kreditkort genom att förse magnetremsorna på plastkort med koder som kunde utläsas i kortläsare och som gav sken av att korten var utfärdade av OKQ8 och kopplade till olika personers konton i företaget, utgjorde urkundsförfalskning enligt 14 kap. 1 § brottsbalken. Högsta domstolens majoritet (3 justitieråd) kom därvid fram till att den omständigheten att det krävdes en maskinell behandling i en kortläsare för att identifiera den skenbara utställaren liksom den kontoinnehavare vars konto skulle belastas, inte fråntog korten deras egenskap av att vara urkunder som har upprättats till bevis. De förfalskade korten var därmed, enligt majoriteten, sådana urkunder som avses i 14 kap. 1 § brottsbalken. Frågan om elektroniska handlingar generellt har urkundsstatus är emellertid inte löst genom rättsfallet.

het, som gör att en handling i elektronisk form inte uppfyller kraven på en urkund och därmed inte heller kan vara ett förfalskningsobjekt. En ändring i urkundsbegreppet, enbart som ett led i en anpassning till konventionen, ansågs emellertid som ett alltför omfattande ingrepp i svensk rätt (Ds 2005:6 s. 223–227). I stället föreslogs att straffansvaret för brukande av något som är förfalskat utvidgades till att omfatta åberopande av en icke autentisk sammanställning av elektronisk data, om den som åberopade denna gav sken av att sammanställningen var autentisk; dvs. ett straffansvar först vid brukande för de fall där den aktuella handlingen inte har urkundskvalitet (Ds 2005:6 s. 227–230).

År 2005 tillsatte regeringen en utredning med uppdrag att göra en översyn av de brott i 14 och 15 kap. brottsbalken som berör urkunden. Översynen skulle syfta till att klarlägga vilka förändringar som kan vara nödvändiga med anledning av utvecklingen av informationsteknologin. Utredningen, som antog namnet It-förfalskningsutredningen, hade att beakta bl.a. artikel 7 i konventionen. I betänkandet *Urkunden i tiden – en straffrättslig anpassning* (SOU 2007:92), föreslog It-förfalskningsutredningen den lagstiftning som ansågs behövas för att undanröja osäkerheten i frågan i vilken uträckning handlingar i elektronisk miljö har urkundsstatus i den mening som avses i brottsbalken.

Regeringen överlämnade den 21 februari 2013 proposition 2012/13:74 *Förfalsknings- och sanningsbrotten* till riksdagen. Förslagen i propositionen överensstämmer i huvudsak med It-förfalskningsutredningens. Lagändringarna föreslås träda i kraft den 1 juli 2013. I propositionen föreslås att beteckningen urkund behålls men att begreppet urkund förtydligas när det gäller traditionella handlingar och bevismärken. Vidare föreslås att begreppet utvidgas till elektroniska handlingar.

Med urkund ska enligt regeringens förslag (se prop. 2012/13:74 s. 42–46) i framtiden avses:

- en handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse och originalkaraktär,
- en elektronisk handling som upprättats till bevis eller annars är av betydelse som bevis och som har utställarangivelse som kan kontrolleras på ett tillförlitligt sätt, och

- ett märke som ställts ut till bevis om en persons identitet eller om en viss rättighet eller prestation och som har originalkaraktär (bevismärke).

För elektroniska handlingar krävs således för urkundsstatus enligt regeringens förslag, utöver att de är av betydelse som bevis, att de har utställarangivelse som kan kontrolleras på ett tillförlitligt sätt.

Regeringen har mot den bakgrunden lämnat följande förslag till ny lydelse av 14 kap. 1 § brottsbalken:

> Den som obehörigen, genom att skriva eller på liknande sätt ange en annan persons namn eller på annat sätt, framställer en falsk urkund eller ändrar eller fyller ut en äkta urkund döms, om åtgärden innebär fara i bevishänseende, för *urkundsförfalskning* till fängelse i högst två år.
>
> Med urkund avses
>
> 1. en handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse och originalkaraktär,
> 2. en elektronisk handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt, och
> 3. ett märke som ställts ut till bevis om en persons identitet eller om en viss rättighet eller prestation och som har originalkaraktär (bevismärke).

Som framgått, avser konventionens artikel om datorrelaterad förfalskning att straffbelägga olika former av manipulation av datorbehandlingsbara uppgifter så att det uppstår icke autentiska uppgifter som kan användas som vilseledande bevis i rättsliga sammanhang. Villfarelsen i fråga om autenticitet ska i vart fall avse den som uppgifterna påstås härröra från.

Som framgått är det oklart i vilken utsträckning svensk rätt i dag uppfyller konventionens krav. Det finns en möjlighet att uppställa krav på att straffansvar ska inträda först om det konstateras att gärningsmannen har haft uppsåt till bedrägeribrott eller annat liknande uppsåt. I dessa fall bör förfarandet enligt svensk rätt kunna vara att betrakta som förberedelse eller försök till exempelvis bedrägeri (se också avsnitt 5.3.9).

Regeringens förslag till ett nytt urkundsbegrepp innebär att det handlande som ska vara straffbelagt enligt konventionens artikel 7 i svensk rätt blir straffbart som urkundsförfalskning. Förslagets krav på att det ska finnas en utställarangivelse för att en elektronisk handling ska kunna tillerkännas urkundsstatus är förenligt med konven-

tionsartikeln. Det är vår bedömning att om regeringens förslag antas av riksdagen, kommer svensk rätt att uppfylla konventionens krav på vad som ska vara straffbelagt som datorrelaterad förfalskning. Möjligheten enligt konventionen att kräva ytterligare rekvisit i form av krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar ska gälla, behöver då inte utnyttjas.

5.3.9 Datorrelaterat bedrägeri (artikel 8)

Bedömning: Svensk rätt uppfyller genom främst bestämmelsen om s.k. datorbedrägeri konventionens krav på vad som ska vara straffbelagt som datorrelaterat bedrägeri.

Skälen för bedömningen

Enligt *artikel 8* ska det vara straffbart som datorrelaterat bedrägeri att förorsaka en annan person förlust av egendom genom att *antingen* mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter *eller* störa ett datorsystems drift, med bedrägligt eller annat brottsligt uppsåt och därigenom orättmätigt skaffa sig själv eller annan person en ekonomisk förmån. Det förutsätts att gärningen begås uppsåtligen och orättmätigt.

Artikeln avser att straffbelägga alla former av otillbörliga ingrepp i datorbehandlingsbara uppgifter eller datorsystems drift som har till syfte att få till stånd en illegal förmögenhetsöverföring (se den förklarande rapporten p. 86). Det centrala i bestämmelsen är att en annan person orsakas förlust av egendom till följd av gärningen och att gärningen begås med uppsåt att skaffa gärningsmannen själv eller en annan person en ekonomisk förmån (se den förklarande rapporten p. 88).

I svensk rätt döms den för *bedrägeri* 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 (9 kap. 1 § första stycket brottsbalken).

För bedrägeri (s.k. datorbedrägeri) döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande

automatiserad process, så att det innebär vinning för gärningsmannen och skada för någon annan (9 kap. 1 § andra stycket brottsbalken).

Bestämmelsen om datorbedrägeri ställer inte upp något krav på att en fysisk person har blivit vilseledd till en viss disposition. Brottet föreligger när någon olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, om förfarandet innebär vinning för gärningsmannen och skada för någon annan (prop. 1985/86:65 s. 43). Någon bestämd krets av skadelidande anges inte, varför det inte behöver utredas vem som har drabbats av skadan (prop. 1985/86:65 s. 43). Den brottsliga handlingen kan bestå i att gärningsmannen lämnar en oriktig eller ofullständig uppgift som ska ligga till grund för en automatisk informationsbehandling. Uppgiften kan lämnas antingen direkt av gärningsmannen till den anläggning som ska behandla informationen, t.ex. en dator, eller så kan vilseledande uppgifter lämnas till någon fysisk person som är inblandad i processen. Ett annat i bestämmelsen särskilt angett tillvägagångssätt är att ändra i program, dvs. i instruktionerna för den automatiska informationsbehandlingen. Slutligen upptas i bestämmelsens exemplifiering av möjliga metoder att begå datorbedrägeri, att olovligen ändra i en upptagning för automatisk informationsbehandling. I första hand tar exemplet sikte på olovliga förfaranden med datorer. Vad som därvid främst avses är att lagrade data olovligen ändras eller helt eller delvis utplånas eller att nya data olovligen förs in i det material som ska bearbetas (prop. 1985/86:65 s. 44). Av brottsbeskrivningen framgår att de angivna exemplen på hur gärningen kan förövas inte utgör någon uttömmande uppräkning av alla slags tänkbara förfaranden. Det avgörande för om bedrägeri föreligger enligt bestämmelsen är om en oriktig förmögenhetsöverföring kommit till stånd till följd av att gärningsmannen på något sätt olovligen ingripit i den automatiska informationsbehandlingen och därigenom påverkat det slutliga resultatet (prop. 1985/86:65 s. 44).

Straffet för bedrägeri är fängelse i högst två år. Är brottet grovt döms för *grovt bedrägeri* till fängelse lägst sex månader och högst sex år (9 kap. 3 § brottsbalken). Vid bedömningen av om brottet är grovt ska särskilt beaktas om gärningsmannen missbrukat allmänt förtroende eller begagnat falsk handling eller vilseledande bokföring eller om gärningen annars varit av särskild farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.

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 § brottsbalken).

Försök och förberedelse till bedrägeri och grovt bedrägeri är straffbart (9 kap. 11 § brottsbalken). Bedrägligt beteende är inte straffbelagt på dessa stadier.

Sedan den 1 augusti 2007 finns vidare en särskild lag om bidragsbrott, bidragsbrottslagen (2007:612). Lagen gäller sådana bidrag, ersättningar, pensioner och lån för personligt ändamål som enligt lag eller förordning beslutas av Försäkringskassan, Pensionsmyndigheten, Centrala studiestödsnämnden, Migrationsverket, Arbetsförmedlingen, kommunerna eller arbetslöshetskassorna (1 §). För *bidragsbrott* döms den som lämnar oriktiga uppgifter eller inte anmäler ändrade förhållanden som han eller hon är skyldig att anmäla enligt lag eller förordning, och på så sätt orsakar fara för att en ekonomisk förmån felaktigt betalas ut eller betalas ut med ett för högt belopp (2 §). För straffansvar ska samtliga objektiva brottsförutsättningar täckas av uppsåt (enligt 5 § kan emellertid grovt oaktsamma förfaranden straffas som *vårdslöst bidragsbrott*). Straffet är fängelse i högst två år eller, om brottet är ringa, böter eller fängelse i högst sex månader. Straffet för grovt bidragsbrott är fängelse lägst sex månader och högst fyra år (3 §). Eftersom bestämmelsen om bidragsbrott är konstruerat med ett farerekvisit är försök till brottet inte kriminaliserat.

Det handlingsrekvisit som anges i bestämmelsen om bidragsbrott är att någon lämnar en oriktig uppgift. Sättet för uppgiftslämnandet har ingen betydelse för bestämmelsens tillämplighet. Bestämmelsen omfattar således såväl skriftliga som muntliga uppgifter. Även felaktiga uppgifter som lämnas elektroniskt över exempelvis internet eller genom servicetelefon kan medföra straffansvar (prop. 2006/07:80 s. 95). I konkurrenshänseende har bestämmelsen genom de speciella brottsförutsättningar som ställs upp företräde framför bedrägeribestämmelsen (grundsatsen om *lex specialis*). Om bidragsbrottslagen är tillämplig, ska alltså bedrägeribestämmelsen inte tillämpas (prop. 2006/07:80 s. 80 och 96). Det förfarande som enligt konventionen ska vara straffbelagt som datorrelaterat bedrägeri skulle således i vissa fall kunna vara att anse som bidragsbrott i svensk rätt.

Såväl den svenska bestämmelsen om datorbedrägeri som artikel 8 förutsätter att gärningen begås med *uppsåt*. Begreppet *orättmätigt* i artikeln får anses motsvara begreppet *olovligen* i datorbedrägeribestämmelsen. Det handlande som ska vara straffbelagt enligt arti-

kel 8 – att åstadkomma förmögenhetsöverföring genom att med olika olovliga åtgärder påverka datorbehandlingsbara uppgifter eller störa ett datorsystems drift – täcks av bestämmelsen om datorbedrägeri.

Enligt vår bedömning motsvarar således den svenska bestämmelsen om datorbedrägeri konventionens krav på vad som ska vara straffbelagt som datorrelaterat bedrägeri. Motsvarande bedömning gjordes i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6 s. 106–107). Som nämnts, kan även vissa av de förfaranden som enligt konventionen ska straffbeläggas som datorrelaterat bedrägeri i svensk rätt vara att anse som bidragsbrott i stället för bedrägeri.

5.3.10 Brott som hänför sig till barnpornografi (artikel 9)

Bedömning: Svensk rätt uppfyller genom bestämmelsen om barnpornografibrott konventionens krav på vad som ska vara straffbelagt som brott som hänför sig till barnpornografi.

Skälen för bedömningen

Enligt *artikel 9* ska olika former av befattning med barnpornografi vara straffbart, när gärningen begås uppsåtligen och orättmätigt. Det ska således (enligt artikel 9.1) vara straffbart att

- *framställa* barnpornografi i syfte att sprida den med hjälp av datorsystem,
- *bjuda ut* eller *tillgängliggöra* barnpornografi med hjälp av datorsystem,
- *sprida* eller *överföra* barnpornografi med hjälp av datorsystem,
- *anskaffa* barnpornografi åt sig själv eller någon annan med hjälp av datorsystem, och
- *inneha* barnpornografi i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter.

Med *barnpornografi* i artikelns mening avses (enligt artikel 9.2) 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 handlande med uttrycklig sexuell innebörd, och
- *realistiska bilder som föreställer en minderårig* som ägnar sig åt handlande med uttrycklig sexuell innebörd.

Med *minderårig* i artikelns mening avses (enligt artikel 9.3) *alla personer under 18 år*. En lägre åldersgräns för begreppet får dock tillämpas, som lägst 16 år.

Barnpornografi i konventionens mening kan alltså bestå av tre olika typer av material. Den första typen utgörs av en skildring av ett sexuellt övergrepp mot ett ”verkligt” barn, den andra av en skildring av en person som ser ut att vara ett barn som ägnar sig åt handlande med uttrycklig sexuell innebörd och den tredje av bilder, som fastän de är realistiska, i praktiken inte innebär att ett ”verkligt” barn ägnar sig åt sexuella handlingar (s.k. virtuell barnpornografi).

De olika typerna av förbjudet material avser i viss mån att skydda olika intressen. Den första inriktar sig på att direkt skydda barn mot övergrepp, medan de två senare avser att motverka beteenden som, även om de inte med nödvändighet skadar det barn som förekommer i materialet eftersom det inte behöver finns något sådant verkligt barn, kan uppmuntra till övergrepp mot barn (se den förklarande rapporten p. 101–102).

Med ”en minderårig” avses alltså i första hand en person under 18 år. Med ”en person som ser ut att vara minderårig” avses en person som är över 18 år men som ser ut som ett barn, dvs. som inte är pubertetsutvecklad. Så kallad anspelningspornografi – dvs. när vuxna personer framställs som barn eller förses med olika attribut för att påminna om barn – torde därför inte omfattas av konventionsartikeln. Skrivningen i den förklarande rapporten angående det intresse som den aktuella typen av material avser att skydda, motsäger inte denna tolkning. (Jfr formuleringen ”en verklig människa som ser ut att vara ett barn” i artikel 1 b (ii) i EU:s rambeslut om åtgärder för att bekämpa sexuellt utnyttjande av barn och barnpornografi, vilken enligt regeringens mening var att tolka så att den avsåg en person som är över 18 år men som ser ut som ett barn, varför anspelningspornografi inte ansågs omfattas av rambeslutet, prop. 2003/04:12 s. 32.)

En fördragsslutande stat får (enligt artikel 9.4) förbehålla sig rätten att, helt eller delvis, inte straffbelägga anskaffande eller innehav av barnpornografi och även att inte låta begreppet barnpornografi innefatta en person som enbart ser ut att vara minderårig eller realistiska bilder som föreställer en minderårig.

I svensk rätt döms, enligt 16 kap. 10 a § brottsbalken, den för *barnpornografibrott* som

1. skildrar barn i pornografisk bild,
2. sprider, överlåter, upplåter, förevisar eller på annat sätt gör en sådan bild av barn tillgänglig för någon annan,
3. förvärvar eller bjuder ut en sådan bild av barn,
4. 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
5. innehar en sådan bild av barn eller betraktar en sådan bild som han eller hon berett sig tillgång till.

De olika gärningsformerna omfattar i huvudsak följande beteenden (se prop. 1997/98:43 s. 163–164 samt 2009/10:70 s. 17 och 42–43).

Att *skildra* ett barn i pornografisk bild innebär att en sådan bild av ett barn framställs. En bild kan framställas på olika sätt, t.ex. genom att ett verkligt barn fotograferas, filmas eller tecknas av. Genom olika tekniker kan också mer eller mindre artificiella bilder skapas. För straffansvar krävs inte att bilden föreställer ett verkligt barn, utan även bilder av fiktiva barn omfattas. Nya framställningar kan också skapas genom att redan befintliga skildringar mångfaldigas eller manipuleras, exempelvis genom att filmsekvenser klipps ihop i en annan ordningsföljd eller att en bild av ett barns huvud klipps ihop med bilden av ett annat barns kropp.

Med *spridning* avses alla tänkbara förfaranden genom vilka ett bildinnehåll förmedlas eller görs tillgängligt för andra, dock under förutsättning att bilden gjorts tillgänglig för fler än endast ett fåtal personer. Riktar sig förfarandet till en enstaka person eller en begränsad krets av personer kan det i stället, med hänsyn till omständigheterna, vara fråga om t.ex. straffbar överlåtelse, upplåtelse eller förevisning. Med *överlåtelse* avses att en bild säljs, byts eller skänks bort och med *upplåtelse* att den hyrs eller lånas ut.

Förevisning innebär t.ex. att en person visar en bild eller spelar upp en film för någon annan.

Den gärningsform som består i att någon *förvärvar eller bjuder ut* en barnpornografisk bild träffar främst dem som uppträder som mellanhänder. I övrigt utgör sådana åtgärder ofta led i t.ex. spridning eller överlåtelse.

Att någon *förmedlar kontakter mellan köpare och säljare eller vidtar någon annan liknande åtgärd som syftar till att främja handel med barnpornografiska bilder* innebär att han eller hon vidtar vissa åtgärder som, utan att innefatta befattning med bilderna, är ägnade att öka spridningen av dem. Detta kan t.ex. vara fallet om någon tillhandahåller en lista med adresser till köpare och säljare. Det fordras inte att någon personlig kontakt har uppstått mellan en viss köpare och säljare eller mellan en kontaktförmedlare och en köpare eller säljare. För straffbarhet krävs däremot att förmedlingsverksamheten kan sägas vara satt i system. Det krävs således mer än en enstaka transaktion eller förmedling.

Med *innehav* avses detsamma som i t.ex. narkotikastrafflagen (1968:64), nämligen att i civilrättslig mening ha besittning till något.

Att någon *betraktar* en barnpornografisk bild som han eller hon *berett sig tillgång till* innebär att ansvar för barnpornografibrott kan dömas ut, utan att gärningsmannen innehar bilden. I uttrycket ”bereda sig tillgång till” ligger ett krav på aktivitet och i uttrycket ”betrakta” ligger att gärningsmannen därutöver ska ha tillgodogjort sig bildens innehåll. För straffbarhet krävs att gärningsmannen haft uppsåt dels i förhållande till den omständigheten att de vidtagna åtgärderna innebär att han eller hon berett sig tillgång till bilden och att bildens motiv är sådant att den är att anse som barnpornografisk, dels till att han eller hon betraktat bilden. Har någon oavsiktligen kommit att titta på en barnpornografisk bild är detta alltså inte straffbart.

Utöver nu nämnda gärningsformer är det också straffbart att av oaktsamhet sprida barnpornografiska bilder, om spridningen skett i yrkesmässig verksamhet eller annars i förvärvssyfte.

Straffet för barnpornografibrott är fängelse i högst två år, eller om brottet är ringa, böter eller fängelse i högst sex månader. För grovt barnpornografibrott döms till fängelse lägst sex månader och högst sex år. Försök till barnpornografibrott av normalgraden är straffbart liksom försök eller förberedelse till grovt barnpornografibrott (16 kap. 17 § brottsbalken).

Enligt lagen (1998:1443) om förbud mot införsel och utförsel av barnpornografi är det vidare straffbart att föra en skildring av barn i pornografisk bild in i eller ut ur Sverige. 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 viss 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 ska inte dömas till ansvar. Straffbestämmelsen är subsidiär till reglerna i brottsbalken (7 § andra stycket).

Som framgått av redogörelsen över bestämmelsen om barnpornografibrott är samtliga de *former av befattning* med barnpornografi som ska vara straffbelagda enligt konventionen straffbelagda som barnpornografibrott i svensk rätt. Det kan i sammanhanget konstateras att svensk rätt straffbelägger fler former av befattning med barnpornografi än vad konventionen kräver.

Någon definition av begreppet *pornografisk bild* innehåller bestämmelsen om barnpornografibrott inte. Enligt motiven ska en bild av ett barn, för att vara straffbar, enligt vanligt språkbruk och allmänna värderingar vara pornografisk (prop. 1978/79:179 s. 9 och 1997/98:43 s. 80). Den närmare innebörden av ordet pornografisk i den mening som avses i brottsbalkens bestämmelser anses vara ”en bild, som utan att ha några vetenskapliga eller konstnärliga värden, på ett ohöljt och utmanade sätt skildrar ett sexuellt motiv” (prop. 1970:125 s. 79–80 och 1997/98:43 s. 80). Konventionen överlåter åt den nationella rätten att närmare definiera vad som ska anses utgöra ”pornografiskt material” (se den förklarande rapporten p. 99). I den förklarande rapporten (p. 100) ges exempel på vad som i artikel 9.2 a–c avses med ”handlande med uttrycklig sexuell innebörd”. Det råder inte någon tvekan om att skildringar av sådana handlingar vore att anse som pornografiska i svensk rätt.

Med *barn* avses enligt 16 kap. 10 a § brottsbalken en person vars pubertetsutveckling inte är fullbordad *eller* som är under arton år. Är pubertetsutvecklingen fullbordad ska emellertid ansvar för gärning enligt punkterna 2–5 ovan dömas ut bara om det av bilden och omständigheterna kring den framgår att den avbildade personen är under arton år.

Fram till den 1 januari 2011 var straffbestämmelsen om barnpornografibrott utformad så, att med barn avsågs en person vars pubertetsutveckling inte var fullbordad eller en person som, när det framgick av bilden och omständigheterna kring den, var under 18 år.

För att någon skulle kunna dömas för barnpornografibrott som bestod i befattning med bilder av en fullt pubertetsutvecklad person under 18 år fordrades alltså, även i det fallet att befattningen bestod i att *skildra*, att den avbildade personens ålder framgick av bilden och omständigheterna kring den. I rättstillämpningen hade på många håll därvid antagits att den tilltalades *vetskap* om att den avbildade personen var under 18 år var en sådan ”omständighet kring bilden” som ensam kunde utlösa tillämpning av straffstadgandet (se SOU 2007:54 s. 81). I NJA 2005 s. 80 klargjorde Högsta domstolen emellertid att en sådan tolkning är utesluten. I rättsfallet uttalas att det inte skulle vara förenligt med de tankar som ligger till grund för lagrummets konstruktion att – i en situation då åldern varken framgår av bilden eller presentationen av den – lägga den avbildade personens faktiska ålder och gärningsmannens kännedom om den till grund för straffansvar. I det aktuella avgörandet frikändes den tilltalade därför från ansvar för barnpornografibrott, trots att han framställt pornografiska bilder av fullt pubertetsutvecklade personer och därvid ostridigt vetat om att de var under 18 år.

Lagändringen den 1 januari 2011 innebär att för straffbar *skildring* av en fullt pubertetsutvecklad person under 18 år inte längre krävs att åldern framgår av bilden och omständigheterna kring den. Enligt regeringens mening framstod det inte som försvarbart att den som skildrat en fullt pubertetsutvecklad person i pornografisk bild och då känt till att personen var under 18 år, inte kunde fällas till ansvar för barnpornografibrott (prop. 2009/10:70 s. 25). Det ansågs dock inte finnas tillräckliga skäl att på motsvarande sätt utvidga det straffbara området för övriga former av barnpornografibrott (prop. 2009/10:70 s. 24–25). För t.ex. straffbart innehav krävs alltså även fortsättningsvis att bilden visar en person vars pubertetsutveckling inte är fullbordad eller som, när det framgår av bilden och omständigheterna kring den, är under 18 år. För sådan befattning med barnpornografi som inte består i att skildra, har således det nämnda avgörandet från Högsta domstolen fortsatt relevans.

Som framgått, definierar konventionen termen minderårig som alla personer under 18 år. Efter lagändringen den 1 januari 2011 är den svenska lagstiftningen med säkerhet i överensstämmelse med konventionen när det gäller att *framställa* barnpornografi, eftersom

det straffbara området numer, för den form av barnpornografibrott som består i att *skildra* barn i pornografisk bild, omfattar bilder av personer vars pubertetsutveckling inte är fullbordad *eller* som är under 18 år. När det gäller övriga former av befattning med barnpornografi är läget, som framgått, ett annat. Det skulle således kunna uppstå en situation i vilken någon exempelvis (i ett datorsystem) innehar eller (med hjälp av datorsystem) sprider pornografiska bilder av ett fullt pubertetsutvecklat barn med vetskap om att den som avbildas är under 18 år, men där det samtidigt inte av bilden och omständigheterna kring den framgår att den avbildade personen är under 18 år. En sådan gärning är straffri i svensk rätt, medan definitionen i artikel 9.3 av minderårig omfattar alla under 18 år. Någon möjlighet att generellt förbehålla sig rätten att inte straffbelägga dessa fall erbjuder konventionen inte (förbehåll kan dock lämnas i fråga om gärningsformerna *anskaffande* och *innehav*; se artikel 9.4).

Frågan är om denna skillnad utgör ett hinder mot att tillträda konventionen utan någon begränsning. Ur ett mindre teoretiskt perspektiv kan man fråga sig om det föreligger någon egentlig skillnad mellan vad som är straffbelagt i svensk rätt och vad som ska vara straffbelagt enligt konventionen. Konventionen uppställer endast krav på straff för uppsåtliga gärningar. Gärningsmannens uppsåt måste även omfatta den omständigheten att den person som avbildats är under 18 år. När det gäller andra former av befattning med barnpornografi än framställning (exempelvis spridning och innehav), måste det i praktiken vara omöjligt att styrka att gärningsmannen haft uppsåt i fråga om den avbildades ålder, när den avbildade personen är fullt pubertetsutvecklad och åldern inte framgår av bilden och omständigheterna kring den. Vid sådan befattning har ju gärningsmannen med största sannolikhet inte någon personlig kännedom om och har inte haft någon personlig kontakt med den avbildade. Sådan befattning med barnpornografi som, mot bakgrund av hur den svenska definitionen av barn är konstruerad, inte är straffbelagd i svensk rätt bör normalt inte heller anses belagd med straff enligt konventionen med hänsyn till dess krav på uppsåt.

Bestämmelsen i 16 kap. 10 b § brottsbalken innehåller undantag från det straffbara området i 10 a §. Undantaget i första stycket i 10 b § innebär att förbuden mot skildring och innehav inte gäller den som enligt 10 a §, utan att det rör sig om grovt brott, framställer en pornografisk bild av barn, om skillnaden i ålder och utveckling mellan den avbildade personen och den som framställer bilden är ringa och omständigheterna i övrigt inte påkallar att ansvar

döms ut. Regelns syfte är att från det straffbara området undanta vissa mindre straffvärda fall som har sitt upphov i att barn av oaktsamhet begår barnpornografibrott, exempelvis när två unga människor inom ramen för en varaktig eller tillfällig relation enas om att avbilda sitt sexuella umgänge eller avbildar varandra i samband med sexuell posering (prop. 2009/10:70 s. 37). Det är uteslutande vid *skildring* och vid skildrarens därefter följande *innehav* av den av honom eller henne framställda bilden som det kommer i fråga att på den angivna grunden undanta en gärning från det straffbara området. Som framgått, ställer konventionen krav på att framställande av barnpornografi *i syfte att sprida den med hjälp av datorsystem* straffbeläggs. Att skildra barn i pornografisk bild *i syfte att sprida* bilden är inte en handling som är avsedd att träffas av undantaget i 10 b § första stycket. Vår bedömning är således att svensk rätt, trots undantaget, är förenlig med konventionens krav på kriminalisering av *framställande* av barnpornografi, eftersom det som konventionen avser att kriminalisera i detta avseende undantagslöst är straffbart i svensk rätt. Läget är till synes ett annat när det gäller *innehav* av barnpornografi. Som framgått, kräver konventionen i denna del att det ska vara straffbart att i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter inneha barnpornografi. Den typ av befattning med barnpornografiska bilder som träffas av ansvarsbegränsningsregeln i 10 b § första stycket torde inte sällan bestå i just att inneha bilder i ett datorsystem, exempelvis i en mobiltelefon eller ”vanlig” dator. Enligt vår bedömning är den svenska lagstiftningen ändå förenlig med konventionsåtagandet eftersom den typ av innehav som det är fråga om i dessa undantagsfall i konventionens mening inte kan karaktäriseras som ”orättmätigt”. Allmänt sett gäller också att en konvention av det slag som den aktuella, som ska gälla för stater med olika utformning av sina respektive rättssystem, inte kan tolkas bokstavligt på så sätt att den förvägrar den nationella lagstiftningen att innehålla mer nyanserade regler för utdömande av straffansvar. Vår mening är således inte att den svenska ansvarsbegränsningsregeln i 10 b § första stycket innebär att Sverige (enligt artikel 9.4 jfr med 42) måste förbehålla sig en möjlighet att inte kriminalisera sådant innehav av barnpornografi som träffas av regeln.

Av andra stycket i 10 b § följer att förbuden i 10 a § inte heller gäller den som tecknar, målar eller på något annat liknande hantverksmässigt sätt framställer en sådan bild, om bilden inte är avsedd att spridas, överlåtas, upplåtas, förevisas eller på annat sätt göras till-

gänglig för andra. Undantaget har tillkommit för att inte hindra framställningen av konstnärliga alster och som på grund av framställningstekniken väsentligen kan antas vara framställda för eget bruk (prop. 1997/98:43 s. 162). Med hantverksmässig framställningsform avses förutom målningar och teckningar m.m. t.ex. skulpturer. Undantaget omfattar däremot inte sådana framställningsformer där resultatet enkelt kan komma att omsättas eller spridas. Fotografier omfattas således inte av undantaget och inte heller datorframställda bilder (prop. 1997/98:43 s. 162). Konventionen reglerar inte hantverksmässigt framställda bilder, utan enbart bilder som föreställer verkliga personer och realistiska bilder på fiktiva barn. Av den förklarande rapporten (p. 99) framgår också att konventionen godtar att nationell rätt inte betraktar exempelvis material med konstnärliga värden som ”pornografiskt material” i den mening som avses i artikel 9.2. Vår mening är därför att undantaget i svensk rätt för hantverksmässigt framställda bilder inte är oförenligt med konventionen.

Enligt tredje stycket i 10 b § ska vidare en gärning även i andra fall inte utgöra brott, om gärningen med hänsyn till omständigheterna är *försvarlig*. Undantaget är avsett att träffa situationer där befattning med barnpornografi kan framstå som befogad och där det vore otillfredsställande att helt förlita sig på att de kolliderande intressena ska lösas med en ”livets regel” inom rättstillämpningen (prop. 1997/98:43 s. 91). De fall som här avsetts är de där syftet med gärningen är ”skyddsvärt, konkret och specifikt” och omständigheterna är sådana att det i princip är uteslutet att hantera en situation utan att inneha en viss barnpornografisk skildring, exempelvis inom ramen för massmediernas och frivilligorganisationernas arbete (prop. 1997/98:43 s. 91). Även detta undantag är enligt vår bedömning förenligt med konventionen, eftersom konventionens krav på kriminalisering endast omfattar gärningar som begås *orättmätigt*.

Pornografi i vilken vuxna personer framställs som barn eller som på annat sätt t.ex. genom olika attribut eller roller anspelar på barn, s.k. anspelningspornografi, är inte straffbelagt i svensk rätt. Vi har tidigare gjort bedömningen att anspelningspornografi inte omfattas av vad som ska vara kriminaliserat enligt konventionen, varför den svenska hållningen när det gäller denna form av pornografi inte bedöms stå i konflikt med konventionen.[6]

[6] Vid remissbehandlingen av promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gav några remissinstanser uttryck för uppfattningen att konventionen även avsåg att straff-

Sammanfattningsvis är det vår bedömning att svensk rätt genom bestämmelsen om barnpornografibrott uppfyller konventionens krav på vad som ska vara straffbelagt som brott som hänför sig till barnpornografi.

5.3.11 Brott som hänför sig till intrång i upphovsrätt och till upphovsrätten närstående rättigheter (artikel 10)

Bedömning: Svensk upphovsrättslig lagstiftning uppfyller konventionens krav på vad som ska vara straffbelagt som brott som hänför sig till intrång i upphovsrätt och till upphovsrätten närstående rättigheter. Sverige behöver inte utnyttja möjligheten att göra sådana förbehåll som avses i artikel 10.3.

Skälen för bedömningen

Enligt *artikel 10* ska olika former av intrång i upphovsrätt och till upphovsrätten närstående rättigheter straffbeläggas, om de begås *uppsåtligen*, *i kommersiell skala* och *med hjälp av ett datorsystem*. Ideella rättigheter är undantagna från tillämpningsområdet. De upphovsrätter som avses i artikeln anges genom en hänvisning till vissa upphovsrättsliga konventioner.

För en enskild stat är artikeln inte mer förpliktande än vad som följer av den statens anslutning till respektive konvention. En stat som inte är ansluten till en viss konvention förpliktas alltså inte någonting, såvitt avser intrång i den upphovsrätt som följer av den konventionen. För en stat som visserligen anslutit sig till en viss konvention men därvid gjort visst förbehåll, är förbehållet vidare alltså giltigt även i förhållande till den förpliktelse som följer av artikeln (se den förklarande rapporten p. 110).

En fördragsslutande stat får i begränsad utsträckning förbehålla sig möjligheten att avstå från att införa straffansvar, under förutsättning att andra effektiva rättsliga åtgärder kan komma i fråga och att förbehållet inte avviker från statens internationella förpliktelser enligt de nämnda överenskommelserna (artikel 10.3).

De internationella överenskommelser som räknas upp i artikeln är:

---

belägga anspelningspornografi, varför Sverige enligt dessa, med bibehållen svensk uppfattning att inte kriminalisera denna form av pornografi, borde göra ett förbehåll om detta.

- Paris-beslutet om revidering av Bernkonventionen för skydd för upphovsrätten till litterära och konstnärliga verk,
- Avtalet om handelsrelaterade aspekter av immaterialrätten (TRIP:s-avtalet),
- WIPO[7]-fördraget om upphovsrätt (WCT)[8],
- Romkonventionen om skydd för utövande konstnärer, framställare av fonogram och radioföretag, samt
- WIPO-fördraget om framföranden och fonogram (WPPT)[9].

Bernkonventionen tillkom år 1886 och har sedan dess genomgått flera revisioner. Den första av dessa ägde rum i Berlin år 1908, den andra i Rom år 1928, den tredje i Bryssel år 1948, den fjärde år 1967 i Stockholm och den femte och senaste i Paris 1971. Sverige anslöt sig redan 1904 till den ursprungliga texten från 1886 och har sedan ratificerat de därefter antagna texterna. För svensk del gäller alltså texten i den version som antogs i Paris år 1971. Syftet med konventionen är att så effektivt och enhetligt som möjligt skydda upphovsmännens rättigheter till deras litterära och konstnärliga verk.

Romkonventionen ger utövande konstnärer, framställare av fonogram och andra ljudupptagningar samt radio och televisionsföretag skydd. Konventionen har ratificerats av Sverige och trädde i kraft år 1964.

I samband med att Världshandelsorganisationen (World Trade Organisation, WTO) bildades år 1994 antogs inom organisationen en immaterialrättslig överenskommelse, Avtalet om handelsrelaterade aspekter av immaterialrätter. Avtalet är känt som *TRIP:s-avtalet*. Det har ratificerats av Sverige och trädde i kraft år 1996.

För att anpassa den upphovsrättsliga lagstiftningen till den tekniska utvecklingen har åtgärder under senare år vidtagits på internationell nivå inom bl.a. Världsorganisationen för den intellektuella äganderätten (WIPO) och EU. Arbetet inom WIPO resulterade år 1996 i antagandet av två nya konventioner. Den ena konventionen reglerar upphovsrätten och brukar benämnas *WCT* (WIPO Copyright Treaty eller *WIPO-fördraget om upphovsrätt*) Den andra reglerar vissa till upphovsrätten närstående rättigheter, nämligen skyddet för sångare, musiker eller andra utövande konstnärer när det gäller

[7] WIPO står för Världsorganisationen för den intellektuella äganderätten.
[8] WIPO Copyright Treaty (WCT).
[9] WIPO Performances and Phonograms Treaty (WPPT).

ljudupptagningar av deras framföranden t.ex. på CD-skivor och skyddet för producenter av ljudupptagningar (fonogram), dvs. skivbolag m.fl., och brukar benämnas *WPPT* (WIPO Performances and Phonograms Treaty eller *WIPO-fördraget om framföranden och fonogram*). Syftet med båda konventionerna är att anpassa det internationella regelverket på upphovsrättens område till den digitala utvecklingen, särskilt internet. Inom EU har arbetet bl.a. resulterat i direktiv 2001/29/EG om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället (*upphovsrättsdirektivet*). Ett huvudsyfte med direktivet är att införliva bestämmelserna i WCT och WPPT på ett samordnat sätt inom gemenskapen. Direktivet genomfördes i svensk rätt den 1 juli 2005 (prop. 2004/05:110). Samtliga EU:s medlemsstater tillträdde de båda WIPO-fördragen vid samma tidpunkt år 2009.

Sverige har alltså tillträtt samtliga de konventioner som anges i artikel 10. De straffrättsliga bestämmelser och andra sanktionsregler som överenskommelserna nationellt förutsätter finns i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (URL).

Svensk rätt har under senare år, bl.a. som en följd av tillträdet till de båda WIPO-fördragen, anpassats till den digitala teknikutvecklingen. Upphovsmännens ensamrättigheter har klargjorts och i URL har införts en uttrycklig ensamrätt för upphovsmän att överföra sina verk till allmänheten, oavsett på vilket sätt detta sker. För upphovsrättsintrång straffas den som uppsåtligen eller av grov oaktsamhet på olika sätt, exempelvis med hjälp av ett datorsystem, gör intrång i en upphovsrätt eller en till upphovsrätten närstående rättighet. I svensk rätt krävs för straffansvar inte att intrånget sker i kommersiell skala, även om vissa otillåtna åtgärder med datorprogram och digitala sammanställningar är straffria, om de sker enbart för enskilt bruk. Den svenska lagstiftningen går alltså utöver vad som krävs enligt artikel 10.

Sammanfattningsvis är det vår bedömning att svensk rätt uppfyller konventionens krav på vad som ska vara straffbelagt som brott som hänför sig till intrång i upphovsrätt och till upphovsrätten närstående rättigheter. Något behov av att i enlighet med artikel 10.3 utnyttja möjligheten att uppställa förbehåll i visst avseende torde inte finnas för svensk del.

Motsvarande bedömning av svensk rätts förenlighet med konventionsartikeln gjordes i promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6, s. 116), under förutsättning av att de lagändringar som vid tiden för promemorian föreslagits bl.a. som en följd av det

tidigare nämnda upphovsrättsdirektivet genomfördes. Dessa lagändringar har alltså nu genomförts. Remissinstanserna hade inte några invändningar mot bedömningen.

I sammanhanget bör nämnas att Upphovsrättsutredningen i sitt slutbetänkande *En ny upphovsrättslag* (SOU 2011:32) lämnat förslag till en ny upphovsrättslag som ska ersätta den nuvarande lagen. Förslaget innebär att bestämmelserna i 1960 års upphovsrättslag överförs till den nya upphovsrättslagen, med redaktionella och språkliga förändringar. Det föreslås inte några nya eller ändrade regler i betänkandet utan endast förändringar i språkligt och redaktionellt hänseende.[10] Utredningens förslag bereds för närvarande i Regeringskansliet.

5.3.12 Försök och medhjälp (artikel 11)

Bedömning: Svensk rätt uppfyller konventionens krav på kriminalisering av medhjälp och försök till brotten i artiklarna 2–10.

Skälen för bedömningen

Enligt *artikel 11.1* ska *medhjälp* till samtliga brott i artiklarna 2–10 vara straffbart.

I svensk rätt ådöms, enligt den allmänna medverkansbestämmelsen i 23 kap. 4 § brottsbalken, straffansvar inte bara den som utfört gärningen utan även annan som har främjat denna med råd eller dåd. Regeln gäller vid alla brottsbalksbrott samt de brott i specialstraffrätten för vilka fängelse är föreskrivet eller för vilka särskild föreskrift finns att medverkan ska bestraffas (23 kap. 4 § första och fjärde styckena brottsbalken, se även Berggren m.fl., *Brottsbalken En kommentar Kap. 13–24*, s. 23:50).

Den som inte är att anse som gärningsman döms för anstiftan om han eller hon har förmått annan att utföra brottet. I övriga fall döms för medhjälp till brottet. Varje medverkande ska bedömas efter det uppsåt eller den oaktsamhet som han eller hon har visat.

[10] Förslagen omfattar dock de ändrade eller helt nya bestämmelser som framgår av utredningens förslag i delbetänkandet *Avtalad upphovsrätt* (SOU 2010:24). Utredningens uppdrag var i denna del att göra en allsidig översyn av bestämmelserna om upphovsrättens övergång i 3 kap. URL och att se över vissa frågor om avtalslicenser m.m. Vidare föreslås att samtliga bestämmelser i internationella upphovrättsförordningen (1994:193) tas in i den nya upphovsrättslagen.

I svensk rätt är anstiftan av och medhjälp till samtliga de brott som vi i avsnitt 5.3.3–5.3.11 ansett motsvara de brott som upptas i artiklarna 2–10 straffbart.

Enligt *artikel 11.2* ska *försök* till brott enligt artiklarna 3 (olaglig avlyssning), 4 (datastörning), 5 (systemstörning), 7 (datorrelaterad förfalskning,) 8 (datorrelaterat bedrägeri) samt 9.1 a och 9.1 c (barnpornografibrott som består i att framställa barnpornografi i syfte att sprida den med hjälp av ett datorsystem och att sprida eller överföra barnpornografi med hjälp av ett datorsystem) vara straffbelagt. I *artikel 11.3* finns en möjlighet för en anslutande stat att förbehålla sig rätten att, helt eller delvis, inte straffbelägga brotten på försöksstadiet.

Vi har i tidigare avsnitt gjort bedömningen att svensk rätt uppfyller konventionens krav på kriminalisering av de nämnda brotten främst genom bestämmelserna om dataintrång, brytande av post- eller telehemlighet, skadegörelse, sabotage, urkundsförfalskning (under förutsättning av att regeringens förslag till ett nytt urkundsbegrepp antas av riksdagen), datorbedrägeri och barnpornografibrott.

Försök till dataintrång är straffbart under förutsättning att intrånget inte skulle ha varit att anse som ringa om det hade fullbordats. Försök till bedrägeri, grovt bedrägeri, urkundsförfalskning, grov urkundsförfalskning, barnpornografibrott och grovt barnpornografibrott är straffbart, medan försök till bedrägligt beteende, förvanskning av urkund och ringa barnpornografibrott inte är det. Eftersom konventionen inte kräver att ringa fall av de fullbordade brotten i artiklarna 3, 4, 5, 7, 8 och 9 straffbeläggs (se den förklarande rapporten p. 37 och avsnitt 5.3.1), är det enligt vår mening en rimlig tolkning att utgå ifrån att så inte heller krävs i fråga om försök i sådana fall, även om de fullbordade ringa gärningarna i och för sig kriminaliseras i nationell rätt. Möjligheten att avge förbehåll torde därför inte behöva utnyttjas för dessa ringa brottsformer.

När det gäller skadegörelse, grov skadegörelse, sabotage och grovt sabotage är försök till dessa brott straffbelagda. Försök till brytande av post- eller telehemlighet är inte straffbart. Däremot är, som nämnts i avsnitt 5.3.4, förberedelse till brytande av telehemlighet straffbar genom en särskild bestämmelse i 4 kap. 9 b § brottsbalken. Om någon anbringar ett tekniskt hjälpmedel med uppsåt att bryta telehemlighet ska han dömas för förberedelse till sådant brott, under förutsättning att han inte har gjort sig skyldig till fullbordat brott. Skälet till att denna lösning för osjälvständiga brottsformer av detta brott har valts är att det ansetts vara svårt att bevisa att apparatur

som påträffas under sådana omständigheter, att man kan utgå från att den som har anbringat den har haft uppsåt att avlyssna, verkligen har använts för detta ändamål (prop. 1975:19 s. 86). Straffbestämmelsen i 4 kap. 9 b § torde uppfylla konventionens krav på kriminalisering i stadierna före fullbordat brott.

Sammanfattningsvis gör vi bedömningen att svensk rätt uppfyller konventionens krav på kriminalisering av medhjälp och försök till brotten i artiklarna 2–10.

5.3.13 Juridiska personers ansvar (artikel 12)

Bedömning: Svensk rätt får genom bestämmelserna om företagsbot och förverkande anses uppfylla de krav som konventionen ställer i fråga om ansvar för juridiska personer.

Skälen för bedömningen

Enligt *artikel 12* ska även juridiska personer kunna hållas ansvariga för brott som ska straffbeläggas enligt konventionen. För att juridiska personer ska kunna hållas ansvariga måste, enligt *punkt 1*, fyra förutsättningar vara uppfyllda (se den förklarande rapporten p. 124). För det *första* måste något av brotten i artiklarna 2–11 ha begåtts. För det *andra* måste det brottet ha begåtts till förmån för den juridiska personen eller på dennas vägnar. För det *tredje* måste en person i ledande ställning ha agerat och för det *fjärde* måste denna person ha agerat med stöd av antingen en fullmakt att företräda den juridiska personen eller en befogenhet att antingen fatta beslut på den juridiska personens vägnar eller att utöva kontroll inom den juridiska personen.

Enligt *punkt 2* ska ansvar även kunna utkrävas när bristande övervakning eller kontroll som ska utföras av en sådan fysisk person som avses i den första punkten har gjort det möjligt för en fysisk person, som handlar på den juridiska personens vägnar (exempelvis en arbetstagare), att begå brott som straffbeläggs enligt konventionen till förmån för den juridiska personen.

Enligt *punkt 3* står det en fördragsslutande stat fritt att välja vilken typ av ansvar för juridiska personer som ska ställas upp: straffrättsligt, civilrättsligt eller administrativt. Det är alltså inte nödvändigt att införa ett straffrättsligt ansvar för juridiska personer. Av artikel 13.2

framgår dock att sanktionerna måste vara effektiva, proportionella och avskräckande, samt innefatta ekonomiska påföljder.

Juridiska personer kan inte ställas till svars för brott eller ådömas straff enligt svensk rätt. Däremot kan en näringsidkare, även en juridisk person, åläggas företagsbot enligt reglerna i 36 kap. 7–10 a §§ brottsbalken. Företagsbot hanteras inom ramen för det straffrättsliga systemet, men utgör inte ett straff eller en påföljd för brott, utan en särskild rättsverkan av brott. Företagsbot kan åläggas vid brott som har begåtts i utövningen av näringsverksamhet, om det för brottet är föreskrivet strängare straff än penningböter. Därtill krävs

1. att det kan visas att näringsidkaren inte har gjort vad som skäligen kunnat krävas för att förebygga brottsligheten, eller
2. att brottet har begåtts av
   a. en person i ledande ställning grundad på befogenhet att företräda näringsidkaren eller att fatta beslut på näringsidkarens vägnar, eller
   b. en person som annars haft ett särskilt ansvar för tillsyn eller kontroll i verksamheten.

Punkt 1 tar sikte på fall där näringsidkaren som sådan kan anses ansvarig för brottsligheten, t.ex. på grund av att denne har haft bristande rutiner och kontroller till förebyggande av brott. I punkt 2 avses sådana fall där näringsidkaren kan ha haft fullt godtagbara rutiner för att förebygga brottsligheten men där sådana som har ett särskilt ansvar inom företaget har begått brottet (prop. 2005/06:59 s. 60). Med begreppet person i ledande ställning avses framför allt en person som, på grund av att han eller hon ingår i företagets ledning eller under självständigt ansvar rapporterar direkt till ledningen, kan sägas ha ett särskilt ansvar för att verksamheten bedrivs på ett lagenligt sätt. Uttrycket person som annars haft ett särskilt ansvar för tillsyn eller kontroll tar sikte på personer som har ansvar för att kontrollera och utöva tillsyn över att regler (såväl allmänna som näringsidkarens egna), rutiner och säkerhetsföreskrifter upprätthålls och följs i verksamheten (prop. 2005/06:59 s. 61). Med näringsidkare avses, liksom i annan lagstiftning, fysiska eller juridiska personer som yrkesmässigt driver verksamhet av ekonomisk art, oavsett om den är inriktad på vinst eller inte (prop. 1985/86:23 s. 24).

Enligt 36 kap. 8 § brottsbalken ska företagsboten fastställas till lägst fem tusen kronor och högst tio miljoner kronor. När storleken av företagsbot bestäms ska enligt 9 § samma kapitel, med beaktande av straffskalan för brottet, särskild hänsyn tas till den skada eller fara som brottsligheten inneburit samt till brottslighetens omfattning och förhållande till näringsverksamheten. Under vissa speciella förutsättningar som anges i 10 § får företagsboten sättas ned eller helt efterges.

Förutom åläggande av företagsbot kan, enligt 36 kap. 4 § brottsbalken, värdet av ekonomiska fördelar som uppkommit för näringsidkare vid brott i näringsverksamhet förklaras förverkat.

Bestämmelser med motsvarande lydelse som artikel 12 i konventionen finns framför allt i flera gemenskapsrättsliga instrument, t.ex. i en rad rambeslut som antagits inom ramen för samarbetet i rättsliga och inrikes frågor i EU. Riksdagen och regeringen har i flera lagstiftningsärenden som avsett genomförande av dessa rambeslut i svensk rätt ansett att reglerna om företagsbot är tillräckliga för att uppfylla de krav på sanktioner mot juridiska personer som ställts i dessa rambeslut (se t.ex. prop. 2003/04:12 s. 38, 2005/06:209 s. 39, 2006/07:66 s. 31 och 2008/09:25 s. 29). En motsvarande bestämmelse som den i artikel 12 finns också i exempelvis Europarådets konventioner om förebyggande av terrorism (ETS 196) och om bekämpande av människohandel (CETS 197), vilka konventioner Sverige har tillträtt. Reglerna om företagsbot har i lagstiftningsärenden hänförliga till dessa konventioner ansetts tillräckliga för att uppfylla konventionernas krav på ansvar för juridiska personer (prop. 2009/10:78 s. 33–34 och 2009/10:152 s. 46) I det sist nämnda lagstiftningsärendet hänvisades i sammanhanget även till reglerna om förverkande i 36 kap. 4 § brottsbalken.

Konventionen innebär, som nämnts, inte något krav på att sanktionerna mot juridiska personer ska ha någon speciell form så länge som de är effektiva, proportionella och avskräckande. De svenska bestämmelserna om företagsbot och förverkande uppfyller enligt vår bedömning konventionens krav i dessa hänseenden.

5.3.14 Påföljder och åtgärder (artikel 13)

Bedömning: Svensk rätt uppfyller de krav som ställs i konventionen i fråga om påföljder och åtgärder.

Skälen för bedömningen

Enligt *artikel 13.1* ska de fördragsslutande staterna se till att brotten i artiklarna 2–11 straffbeläggs med effektiva, proportionella och avskräckande påföljder, innefattande frihetsberövande. Varken i konventionen eller i den förklarande rapporten anges vad som är att betrakta som en effektiv och avskräckande påföljd i konventionens mening.

De straffskalor som gäller för de brott som i svensk rätt är av relevans för konventionens del, har redovisats i avsnitt 5.3.3–5.3.11. Samtliga dessa brott har fängelse i straffskalan. Mot den angivna bakgrunden gör vi bedömningen att svensk rätt uppfyller kraven i artikel 13.1.

Enligt *artikel 13.2* ska de fördragsslutande staterna se till att sanktioner som åläggs juridiska personer är effektiva, proportionella och avskräckande samt innefattar ekonomiska påföljder. I avsnitt 5.3.13 har vi gjort bedömningen att de svenska bestämmelserna om företagsbot och förverkande får anses uppfylla konventionens krav på sanktioner mot juridiska personer, varför det här hänvisas till detta avsnitt.

5.4 Processrättsliga bestämmelser

5.4.1 Allmänt om bestämmelserna

Konventionens processrättsliga bestämmelser är indelade i avsnitt med utgångspunkt i typen av åtgärd. Den processrättsliga delen inleds emellertid med bestämmelser som är gemensamma för hela den processrättsliga delen (artiklarna 14 och 15). Därefter följer avsnitt om skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter (artiklarna 16 och 17), skyldighet att lämna uppgifter (artikel 18), husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter (artikel 19) samt insamling i realtid av datorbehandlingsbara uppgifter (artiklarna 20 och 21).

5.4.2 De processrättsliga bestämmelsernas räckvidd (artikel 14)

Artikel 14 innehåller bestämmelser om tillämpningsområdet för de processrättsliga reglerna och vilka förbehåll som får göras beträffande dessa.

Enligt *punkt 1* åligger det en fördragsslutande stat att vidta de åtgärder – lagstiftningsmässiga eller andra – som krävs för att se till att de befogenheter och förfaranden som föreskrivs i konventionens processrättsliga bestämmelser kan användas vid brottsutredningar och rättsliga förfaranden.

Av *punkt 2* framgår att de befogenheter och förfaranden som föreskrivs i de processrättsliga bestämmelserna ska tillämpas på de brott som straffbeläggs i enlighet med konventionen, andra brott som begåtts med hjälp av ett datorsystem och insamling av bevis i elektronisk form om ett brott. Avsikten är att det, oavsett vilket brott det är fråga om, ska vara möjligt att insamla och använda digital bevisning eller annan form av elektroniskt bevismaterial samt att denna form av bevisning ska ges samma ställning som konventionellt bevismaterial (se den förklarande rapporten p. 141).

Från den fastlagda huvudregeln i punkt 2 finns emellertid *två undantag*. Det *första* innebär att de tvångsmedel som avses i artikel 21, vilken gäller avlyssning av *innehållsuppgifter*, kan begränsas till att gälla enbart vissa allvarliga brott. Det *andra* framgår av *punkt 3 a*, och innebär att en fördragsslutande stat får förbehålla sig rätten att endast tillämpa de åtgärder som avses i artikel 20, vilken gäller insamling i realtid av *trafikuppgifter*, 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 staten tillämpar de åtgärder som avses i artikel 21. De nu aktuella tvångsmedlen (avlyssning av innehållsuppgifter och insamling i realtid av trafikuppgifter) anses vara av sådan karaktär att de i högre utsträckning än andra i konventionen upptagna tvångsmedel utgör ett integritetsintrång, särskilt gäller det avlyssning av innehållsuppgifter (se den förklarande rapporten p. 142 och 143).

Enligt *punkt 3 b* får en fördragsslutande stat förbehålla sig rätten att inte tillämpa de åtgärder som avses i artiklarna 20 och 21 på meddelanden som överförs inom en tjänsteleverantörs datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte heller är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt (se artikel 1 c och av-

snitt 5.2 om vad som avses med begreppet tjänsteleverantör enligt konventionen). Punkten ger alltså en stat som i sin nationella lagstiftning inte tillåter avlyssning av innehållsuppgifter eller insamling i realtid av trafikuppgifter i fristående slutna nät (exempelvis ett nät som möjliggör för anställda inom samma företag att kommunicera med varandra men inte med andra) en möjlighet att göra förbehåll om detta (se den förklarande rapporten p. 144).

I samtliga konventionens processrättsliga bestämmelser (artiklarna 16–21) finns uttryckligen angivet att bestämmelserna i artikel 14 är tillämpliga på de befogenheter och förfaranden som avses i respektive artikel.

5.4.3 Villkor och garantier (artikel 15)

Artikel 15 innehåller bestämmelser som syftar till att garantera rättssäkerheten vid införandet och användningen av de tvångsmedel och andra åtgärder som konventionen ålägger de fördragsslutande staterna att införa.

I *punkt 1* föreskrivs att de fördragsslutande staterna vid införandet, genomförandet och tillämpningen av konventionens processrättsliga befogenheter och förfaranden ska iaktta proportionalitetsprincipen och även i övrigt se till att de villkor och garantier som i den nationella lagstiftningen sätts upp för användningen av åtgärderna tillgodoser de mänskliga fri- och rättigheterna, däribland de rättigheter som följer av internationella fördrag om mänskliga rättigheter.

Enligt *punkt 2* ska den nationella lagstiftningens villkor och garantier för användningen av viss åtgärd, utifrån vad som är lämpligt med hänsyn till den specifika åtgärden, bl.a. innefatta rättslig eller annan oberoende tillsyn, de skäl som motiverar tillämpningen samt begränsning av omfattningen och varaktigheten av åtgärden.

Enligt *punkt 3* ska även tredje mans rättigheter, skyldigheter och rättmätiga intressen, i den utsträckning det är förenligt med allmänintresset, beaktas vid användningen av konventionens processrättsliga åtgärder. En sådan tredje man som avses i punkten kan exempelvis vara en leverantör (se den förklarande rapporten p. 148).

I samtliga konventionens processrättsliga bestämmelser (artiklarna 16–21) finns uttryckligen angivet att bestämmelserna i artikel 15 är tillämpliga på de befogenheter och förfaranden som avses i respektive artikel.

5.4.4 Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter (artikel 16)

Bedömning: Det krävs lagstiftning för att uppfylla konventionens krav på skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter.

Skälen för bedömningen

Artikel 16 innehåller bestämmelser om skyldighet att *säkra* datorbehandlingsbara uppgifter. Tanken är att det i den nationella lagstiftningen ska finnas moderna och smidiga metoder för säkrande av sådana uppgifter (se den förklarande rapporten p. 155).

Såväl artikel 16 som 17 gäller enbart *lagrade* uppgifter, alltså uppgifter som redan finns samlade och bevarade hos exempelvis en leverantör (se den förklarande rapporten p. 149). I den förklarande rapporten (p. 151) görs en distinktion mellan *lagring av uppgifter* (”*data retention*”) och *säkrande av uppgifter* (”*data preservation*”). Med att säkra uppgifter avses att förvara uppgifter, som redan finns lagrade, på ett sådant sätt att de skyddas från varje form av påverkan som skulle kunna få dem att ändras eller försämras i kvalitet eller skick. Med att lagra uppgifter avses däremot enbart att fortsätta förvara uppgifter som mottagits, utan vidare krav på att de lagrade uppgifterna förvaras på ett säkert och tryggt sätt.

Enligt *punkt 1* ska behöriga myndigheter i en fördragsslutande stat genom förelägganden eller på liknande sätt skyndsamt kunna säkra särskilt angivna datorbehandlingsbara uppgifter, däribland trafikuppgifter, som har lagrats med hjälp av ett datorsystem. Säkrande är viktigt speciellt i de fall där det finns anledning att förmoda att de datorbehandlingsbara uppgifterna löper särskild risk att gå förlorade eller förändras.

Begreppet *trafikuppgifter* definieras i artikel 1 d som ”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”. Med uppgifter som anger typ av underliggande tjänst avses om det vid kommunikation är fråga om t.ex. e-post, filöverföring eller chatt. För konventionens definition av begreppen *datorbehandlingsbara uppgifter* och *datorsystem*, se avsnitt 5.2.

Redan här kan nämnas att begreppet trafikuppgift i 6 kap. 1 § LEK definieras som ”uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande”. Vår uppfattning är att det inte råder någon konflikt mellan konventionens definition av begreppet och den svenska definitionen av detsamma.

Säkrandet behöver inte innebära att uppgifterna görs otillgängliga för den som har legitima skäl att använda dem. En fördragsslutande stat får själv bestämma vilket medel för säkrande som ska användas och om uppgifterna även i fortsättningen ska få användas av den som ska säkra dem (se den förklarande rapporten p. 159).

Som framgår av punkten 1 kan en fördragsslutande stat uppfylla artikelns krav genom ett särskilt föreläggande om säkring eller *på annat liknande sätt*. Säkrande kan därför uppfyllas genom exempelvis husrannsakan och beslag. Artikeln uppställer således inte något krav på en fördragsslutande stat att införa en möjlighet att förelägga någon att säkra uppgifter. Samtidigt är avsikten att de fördragsslutande staterna i vart fall ska undersöka möjligheten att i sin nationella lagstiftning införa en typ av föreläggande, eftersom detta kan förutsättas vara dels ett snabbare och effektivare medel för säkrande, dels mindre ingripande för dem som drabbas än exempelvis husrannsakan och beslag (se den förklarande rapporten p. 160).

När det gäller risken att uppgifterna går förlorade eller förändras kan sådan risk, enligt den förklarande rapporten, exempelvis finnas när den typ av uppgifter det är fråga om enligt ett företags praxis vanligtvis raderas efter viss tid eller när uppgifterna lagras på ett mindre säkert sätt. Risken tar således inte främst sikte på att uppgifterna riskerar att försvinna på grund av att den som förvarar uppgifterna är opålitlig. I sådana fall anses det bättre att säkra uppgifterna genom exempelvis husrannsakan eller beslag i stället för genom ett föreläggande (se den förklarande rapporten p. 161).

Punkt 2 gäller själva *föreläggandet* att säkra uppgifter. Den är således enbart tillämplig i det fall en fördragsslutande stat valt att införa en möjlighet till föreläggande i sin nationella lagstiftning. Ett föreläggande att säkra uppgifter ska riktas mot en person som har särskilt angivna lagrade datorbehandlingsbara uppgifter i sin besittning eller under sin kontroll. Personen ska åläggas att bevara uppgifterna orubbade så länge som det behövs, dock högst 90 dagar, i syfte att göra det möjligt för behöriga myndigheter att ta ställning till om uppgifterna behövs för utredningen och om de kan lämnas

ut. En fördragsslutande stat kan välja att föreskriva att ett sådant föreläggande därefter får förnyas.

I sammanhanget bör noteras att artikel 29.7, som gäller ömsesidig rättslig hjälp, innebär att en stat som ansöker om säkring av den anmodade staten ska ges en tidsfrist på minst 60 dagar, efter att säkrandet verkställts, med att komma in med en framställning om husrannsakan, beslag eller liknande säkringsåtgärd för röjande av uppgifterna.

Punkt 3 ålägger en fördragsslutande stat att vidta nödvändiga åtgärder för att se till att de personer som ska bevara de datorbehandlingsbara uppgifterna, under så lång tid som föreskrivs i statens nationella lagstiftning, hemlighåller säkringsåtgärderna.

Syftet med artikel 16 är alltså att på ett snabbt och för de inblandade mindre ingripande sätt än exempelvis husrannsakan och beslag, se till att datorbehandlingsbara uppgifter som kan vara av betydelse som bevis i ett särskilt fall säkras och bevaras under viss tid för att eventuellt i ett senare skede lämnas ut till brottsutredande myndigheter. Bestämmelsen gäller generellt, dvs. såväl hos enskilda som hos leverantörer. Även om ett sådant säkrande och bevarande visserligen kan vara känsligt ur integritetssynpunkt bör påpekas att artikel 16 enbart handlar om att *bevara* uppgifter. Artikeln reglerar inte de brottsbekämpande myndigheternas *tillgång* till uppgifterna, vilket ur integritetssynpunkt måste anses vara mer känsligt än själva bevarandet av uppgifterna.

För svensk del kan först konstateras att det saknas möjlighet att utfärda förelägganden som avses i punkten 2. Vad gäller lagringsskyldighet av elektroniska uppgifter och möjligheten för de brottsbekämpande myndigheterna att hos leverantörer få tillgång till sådana uppgifter som avses i artikel 16 bör nämnas följande.

Vid genomförandet av Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationsnät och om ändring av direktiv 2002/58/EG (*datalagringsdirektivet*) infördes nya bestämmelser i LEK (6 kap. 3 a § och 16 a–16 f §§). Bestämmelserna trädde i kraft den 1 maj 2012 och innebär att *leverantörer* av allmänt tillgängliga kommunikationstjänster eller allmänna kommunikationsnät åläggs en skyldighet att under sex månader *lagra trafik-* och *lokaliseringsuppgifter* liksom uppgifter som behövs för att *identifiera* en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal i de fall uppgifterna enligt andra

bestämmelser får lämnas ut för detta ändamål. Däremot ska uppgifter om *innehållet* i ett elektroniskt meddelande *inte* lagras. De uppgifter som har lagrats får sedan lämnas ut med stöd av 6 kap. 22 § första stycket 2 LEK (vilket innebär att uppgift om abonnemang och som gäller misstanke om brott på begäran ska lämnas ut till åklagarmyndighet, polismyndighet eller annan myndighet som ska ingripa mot brottet) eller enligt ett beslut om hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § rättegångsbalken (se närmare i det följande). Den som är skyldig att lagra uppgifter ska bedriva verksamheten så att uppgifterna utan dröjsmål kan lämnas ut och så att verkställandet av utlämnandet inte röjs. Uppgifterna ska vidare göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand.

När det gäller lagringsskyldigheten enligt LEK och den förpliktelse som följer av artikel 16 kan konstateras bl.a. följande. Lagringsskyldigheten enligt LEK gäller enbart *operatörer* (sådana leverantörer som är anmälningspliktiga enligt 2 kap. 1 § LEK), medan möjligheten att få till stånd säkrande av uppgifter enligt artikeln ska kunna ske såväl hos *operatörer som hos andra personer, fysiska eller juridiska inklusive sådana leverantörer som inte är anmälningspliktiga enligt LEK*. Vidare gäller lagringsskyldigheten enligt LEK *generellt* medan syftet med artikel 16 är att de brottsbekämpande myndigheterna i en *särskild brottsutredning* ska kunna få till stånd att datorbehandlingsbara uppgifter som är av betydelse för utredningen ska bevaras och hållas intakta. Utgångspunkten för säkrandet enligt artikeln skiljer sig alltså från den som gäller för lagring enligt LEK. Lagringsskyldigheten enligt LEK gäller slutligen enbart trafik- och lokaliseringsuppgifter samt uppgifter som behövs för att identifiera en abonnent eller användare, medan uppgifter om *innehållet* i ett elektroniskt meddelande *inte* lagras. Säkrandet enligt artikel 16 ska däremot kunna avse *alla typer av särskilt angivna datorbehandlingsbara uppgifter* som har lagrats med hjälp av ett datorsystem. Skyldigheten att säkra uppgifter enligt artikel 16 omfattar alltså även uppgifter som inte har någon koppling till ett meddelande som har befordrats eller till ett abonnemang.

Även om artikel 16 alltså inte primärt gäller tillgång till eller röjande av uppgifter lämnas här en redogörelse för de svenska reglerna om hemlig avlyssning av elektronisk kommunikation och hem-

lig övervakning av elektronisk kommunikation. Bestämmelser om dessa tvångsmedel finns i 27 kap. rättegångsbalken.[11]

Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett visst telefonnummer eller en annan adress avlyssnas eller tas upp i hemlighet genom ett tekniskt hjälpmedel (27 kap. 18 §). Hemlig avlyssning av elektronisk kommunikation får användas vid förundersökning som avser ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller försök, förberedelse eller stämpling till ett sådant brott, om sådan gärning är belagd med straff, samt vid förundersökning som gäller ett brott med lägre straffminimum, om brottets straffvärde bedöms överstiga fängelse i två år. Ett tillstånd till hemlig avlyssning av elektronisk kommunikation ger också rätt att hämta in sådana övervakningsuppgifter som annars är åtkomliga med stöd av ett tillstånd till hemlig övervakning av elektronisk kommunikation.

Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits eller att sådana meddelanden hindras från att nå fram (27 kap. 19 §).

Uppgifter om *innehållet* i meddelanden omfattas *inte* av detta tvångsmedel. Regleringen innebär i stället att de brottsbekämpande myndigheterna t.ex. kan få uppgifter om vilka hemsidor en abonnent har besökt och mellan vilka e-postadresser kommunikation har skett.

Hemlig övervakning av elektronisk kommunikation får användas vid förundersökning om brott för vilket det inte är föreskrivet

[11] Möjlighet att använda dessa tvångsmedel finns också enligt bl.a. lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott (2008 års utredningslag) och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (2007 års preventivlag) Den först nämnda lagen gäller vid förundersökning angående vissa allmänfarliga brott, brott mot rikets säkerhet och terroristbrott. Brotten är sådana som utreds av Säkerhetspolisen. Enligt den sist nämnda lagen finns möjligheter att använda hemliga tvångsmedel utan att det pågår en förundersökning, om det med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva brottslig verksamhet som innefattar vissa särskilt allvarliga brott. För hemlig tvångsmedelsanvändning enligt dessa båda lagar gäller i viss mån andra förutsättningar än enligt rättegångsbalken. Lagarna har nyligen varit föremål för en översyn, se Utredningens om vissa hemliga tvångsmedel betänkande, *Hemliga tvångsmedel mot allvarliga brott*, SOU 2012:44. Vi bortser i det följande från de möjligheter att använda hemliga tvångsmedel som följer av 2008 års utredningslag och 2007 års preventivlag, eftersom de bedöms vara av relativt liten betydelse för frågan om svensk rätt lever upp till de krav som ställs i konventionen.

lindrigare straff än fängelse i sex månader samt vid förundersökning om dataintrång enligt 4 kap. 9 c § brottsbalken, barnpornografibrott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, narkotikabrott enligt 1 § narkotikastrafflagen (1968:64) eller narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling. Hemlig övervakning av elektronisk kommunikation får också i dessa fall användas vid misstanke om försök, förberedelse eller stämpling, om gärningen är belagd med straff.

Hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation prövas enligt rättegångsbalken av domstol (27 kap. 21 § första stycket). Kan det befaras att inhämtande av rättens tillstånd till hemlig övervakning av elektronisk kommunikation skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden emellertid ges av åklagaren i avvaktan på rättens beslut (27 kap. 21 a §).[12]

För båda slagen av tvångsmedel gäller som huvudregel att de får användas endast om någon är skäligen misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen om brottet. Hemlig övervakning av elektronisk kommunikation får emellertid även äga rum i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Övervakning som innebär att uppgifter hämtas in om meddelanden får dock i detta fall endast avse förfluten tid (27 kap. 20 § andra stycket). Övervakning i detta syfte får vidare endast användas vid förundersökning som avser brott som kan föranleda hemlig avlyssning av elektronisk kommunikation (dvs. det krävs att brottet är av särskilt allvarligt slag, 27 kap. 19 § tredje stycket).

Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet (27 kap. 21 § andra stycket). Tiden kan förlängas på begäran av åklagaren. Åtgärden får avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning 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 ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att

[12] Någon interimistisk beslutanderätt för åklagare vad gäller hemlig avlyssning av elektronisk kommunikation finns för närvarande inte. Utredningen om vissa hemliga tvångsmedel har emellertid i betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) föreslagit att en sådan införs (se SOU 2012:44 s. 720–727). Utredningens förslag bereds för närvarande i Regeringskansliet.

anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

För tvångsmedlen gäller, som vid all tvångsmedelsanvändning, att åtgärden får komma i fråga endast om skälen för åtgärden uppväger det intrång och men som åtgärden innebär för den misstänkte eller något annat motstående intresse (27 kap. 1 § tredje stycket).

Vissa bestämmelser i LEK knyter an till rättegångsbalkens regler om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. I 6 kap. 19 § LEK regleras anpassningsskyldigheten för operatörerna. Bestämmelsen innebär att vissa verksamheter ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas under sådana former att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

LEK innehåller vidare regler om tystnadsplikt (6 kap. 20 §). Av reglerna följer att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till 1) uppgift om abonnemang, 2) innehållet i ett elektroniskt meddelande, eller 3) annan uppgift som angår ett särskilt elektroniskt meddelande, inte obehörigen får föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Enligt lagen gäller dessutom tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångsmedel, nämligen hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och kvarhållande av försändelser (6 kap. 21 §). Reglerna om tystnadsplikt i LEK som gäller uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande och som gäller uppgifter om hemliga tvångsmedel, har företräde framför den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen (se 44 kap. 4 § offentlighets- och sekretesslagen [2009:400]). Rätten att meddela och offentliggöra uppgifter är alltså helt inskränkt i dessa fall.

När det gäller de svenska tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation och det åtagande som följer av artikel 16 kan konstateras bl.a. följande. Tvångsmedlen innebär att de brottsbekämpande myndigheterna bereds tillgång till den information som inhämtats genom avlyssningen eller övervakningen. De är mot den bakgrun-

den omgärdade av strikta regler i fråga om bl.a. under hur lång tid och vid vilka brott de får användas och det krävs domstolsbeslut för deras användning. Som framgått tidigare handlar artikel 16 i stället enbart om att säkra uppgifter på ett snabbt och så lite ingripande sätt som möjligt. Utlämnandet av uppgifterna till brottsbekämpande myndigheter är en senare fråga, vilket kan vara kringgärdat av andra regler än dem som gäller för själva säkrandet hos den som innehar uppgifterna. Tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation har ett annat syfte än åtgärderna enligt artikel 16. Att de svenska tvångsmedlen enbart får användas vid brott av visst allvar innebär också att de inte kan tillämpas i samtliga de fall som den säkrandeåtgärd som avses i artikel 16 ska kunna användas (jfr artikel 14.2). Samtidigt måste sägas att konventionens artikel 15 och den där inskrivna proportionalitetsprincipen innebär att en fördragsslutande stat vid uppfyllandet av de processrättsliga artiklarna, tillåts sätta upp villkor bl.a. vad gäller krav på viss straffskala för användning av de olika processrättsliga åtgärderna.

I svensk rätt kan datorbehandlingsbara uppgifter säkras även genom *beslag*. Enligt 27 kap. 1 § första stycket rättegångsbalken får bl.a. föremål som skäligen kan antas ha betydelse för utredning om brott tas i beslag (s.k. bevisbeslag). Beslag kan endast avse lösa saker. Eftersom elektronisk information har en bärare, exempelvis en dator, en mobiltelefon eller ett fickminne, som är att betrakta som ett föremål och därför kan tas i beslag fungerar emellertid beslagsreglerna även på elektroniska uppgifter. Av 27 kap. 2 § första meningen rättegångsbalken framgår att vissa skriftliga handlingar inte får tas i beslag. Enligt sin ordalydelse gäller beslagsförbudet endast skriftliga handlingar. Vi återkommer till beslagsförbudets räckvidd i fråga om elektroniska handlingar i avsnitt 5.4.7.

Beslag kan användas oberoende av brottets beskaffenhet och det saknar betydelse för frågan om beslag huruvida föremålet ägs eller innehas av annan än den som misstänks för brottet. En förutsättning för beslag är dock att föremålet är tillgängligt när beslutet om åtgärden fattas. Beslagsrätten ger alltså inte någon befogenhet för beslutsfattaren att vidta åtgärder för att söka efter föremål. Som medel för att få fram föremålet kan t.ex. husrannsakan användas. Enligt gällande svensk rätt anses det tillåtet att under en husrannsakan genomsöka en dator. Det krävs då inte något särskilt beslut om husrannsakan för datorn (SOU 1995:47 s. 184 och SOU 2011:45 s. 295–296). Normalt sett är emellertid i dessa situationer en genom-

sökning inte praktiskt möjlig utan att datorn tas i beslag eller att hårddisken kopieras (se SOU 2011:45 s. 296).

Regler om beslutsbehörighet finns i 27 kap. 4 och 5 §§ rättegångsbalken. Enligt 4 § får den som med laga rätt griper eller anhåller en misstänkt eller verkställer häktning, husrannsakan, kroppsvisitation eller kroppsbesiktning ta föremål som därvid påträffas i beslag. I andra fall när föremål påträffas är det förundersökningsledaren eller åklagaren som får besluta om beslag. Vid fara i dröjsmål har polisman samma behörighet. Om någon annan än förundersökningsledaren eller åklagaren har beslutat om och verkställt beslaget ska det anmälas till denne som omedelbart ska besluta om det ska bestå. Enligt 5 § kan även rätten besluta om beslag om föremålet företes inför rätten eller annars är tillgängligt för beslag.

Den som har drabbats av ett beslag kan, enligt 27 kap. 6 § rättegångsbalken, begära rättens prövning av det.

I viss utsträckning kan i svensk rätt även *editionsföreläggande* användas för att få tillgång till elektroniskt lagrad information. I 23 kap. 14 § andra stycket rättegångsbalken anges att undersökningsledare får hos rätten begära föreläggande att skriftligt bevis ska företes. Några särskilda förutsättningar för detta anges inte i bestämmelsen. Närmare regler om editionsföreläggande finns i 38 kap. rättegångsbalken. Enligt 2 § i kapitlet är den som innehar en skriftlig handling som kan antas ha betydelse som bevis skyldig att förete den. Regeln gäller både tvistemål och brottmål.

Enligt sin ordalydelse gäller bestämmelserna om edition bara skriftliga handlingar. Högsta domstolen har emellertid i NJA 1998 s. 829 funnit dem tillämpliga även på elektroniskt lagrad information. I rättsfallet hade begärts att ett bolag skulle föreläggas att förete datautskrifter innehållande utdrag av s.k. statusloggar avseende vissa larmanläggningar. Att de aktuella uppgifterna var lagrade på datamedium utgjorde inte hinder mot att utskrifter avseende uppgifterna gjordes till föremål för edition.

Edition kan alltså begäras av en handling som ännu inte ”existerar” och editionsföreläggandet kan alltså innebära att den som det riktas mot tvingas utföra en del arbete för att ta fram informationen (jfr Fitger, *Rättegångsbalken II*, s. 38:8). I doktrinen har i anslutning till rättsfallet anförts att det är oklart om det går att få tillgång till det digitalt lagrade materialet i annan form än genom utskrifter, men har antagits att så skulle kunna vara fallet (Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 451).

I brottmål gäller att den misstänkte och hans eller hennes närstående är undantagna från editionsskyldighet. Vidare har från editionsskyldigheten gjorts motsvarande undantag som finns i reglerna om beslagsförbud för handlingar vilkas innehåll är sådant att det omfattas av tystnadsplikt som inte bryts av skyldigheten att vittna (se närmare avsnitt 5.4.7). Det finns även vissa andra undantag från editionsskyldigheten.

Något uttryckligt förbud mot editionsföreläggande i den situationen att det i brottmål ännu inte finns någon skäligen misstänkt person finns varken i 23 kap. 14 § eller 38 kap. rättegångsbalken. I NJA 2003 s. 107 klargjorde Högsta domstolen emellertid att editionsplikten förutsätter att någon är skäligen misstänkt. Högsta domstolen anförde i rättsfallet att den grundläggande tanken är att editionsplikten bör ha samma omfattning som vittnesplikten, vilken bl.a. kommer till uttryck i att editionsföreläggande inte får riktas mot den misstänkte eller någon denne närstående. Även för editionsföreläggande bör det därför, enligt Högsta domstolen, vara en förutsättning att förundersökningen kommit så långt att någon är skäligen misstänkt.

Hos en operatör får uppgifter om meddelanden i ett elektroniskt kommunikationsnät inte hämtas in med stöd av husrannsakan, beslag eller editionsföreläggande. Tillgången till sådana uppgifter regleras i stället exklusivt genom bestämmelserna i rättegångsbalken om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. De brottsutredande myndigheterna kan alltså inte använda editionsföreläggande eller husrannsakan i förening med beslag som substitut för tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Däremot finns i LEK bestämmelser som gör det möjligt att hämta in abonnemangsuppgifter.

När det gäller de svenska bestämmelserna om husrannsakan och beslag samt editionsföreläggande och det åtagande som följer av artikel 16 kan konstateras bl.a. följande. Husrannsakan med efterföljande beslag innebär i och för sig en möjlighet att säkra datorbehandlingsbara uppgifter. Syftet med bestämmelserna i artikeln är emellertid i första hand att tillskapa en snabbare, smidigare och mindre ingripande åtgärd för säkrande än just husrannsakan och beslag. Dessa säkerhetsåtgärder har ursprungligen konstruerats för andra förhållanden och framstår som mindre ändamålsenliga i it-sammanhang. Husrannsakan och beslag kan inte användas för att hos operatörer säkra sådana uppgifter som omfattas av regleringen i 27 kap.

rättegångsbalken, medan den säkringsåtgärd som avses i artikeln ska kunna tillämpas då de aktuella uppgifterna finns lagrade hos såväl operatörer som andra fysiska eller juridiska personer. Ett editionsföreläggande kan inte heller riktas mot operatörer. För editionsföreläggande krävs vidare att det finns någon som är skäligen misstänkt. Artikeln syftar visserligen till att datorbehandlingsbara uppgifter ska kunna säkras redan i ett tidigt skede av en brottsutredning, men något uttryckligt hinder mot att det för säkrande i nationell rätt krävs att det finns någon som är skäligen misstänkt för brottet finns inte. Mot bakgrund av bestämmelserna i artikel 15 kan vi inte se att det skulle anses oförenligt med konventionsåtagandet att exempelvis uppställa krav på viss misstankegrad för att säkrande ska få ske. Editionsföreläggande kräver emellertid ett beslut av domstol, varför det är tveksamt om konventionens krav på skyndsamt säkrande kan åstadkommas genom edition.

Vi gör således bedömningen att de svenska bestämmelserna om operatörers lagringsskyldighet enligt LEK, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, husrannsakan och beslag samt editionsföreläggande inte är tillräckliga för att konventionens krav på skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 16 ska anses uppfyllt.

Som tidigare nämnts innebär konventionens bestämmelser om ömsesidig rättslig hjälp (artikel 29.7) bl.a. att en fördragsslutande stat som anmodar en annan fördragsslutande stat att säkra vissa uppgifter, ska ges en tidsfrist på minst 60 dagar, efter att säkrandet verkställts, med att komma in med en framställning om husrannsakan, beslag eller liknande säkringsåtgärd för röjande av uppgifterna.

Enligt lagen (2000:562) om internationell rättslig hjälp i brottmål (Lirb) får emellertid svensk åklagare exempelvis vidta husrannsakan och verkställa beslag eller hos rätten ansöka om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på begäran av en annan stat först när den andra staten inkommit med en formell ansökan om åtgärden. En ansökan ska, beroende på vilken åtgärd den avser, innehålla vissa uppgifter och i förekommande fall ska vissa dokument bifogas (2 kap. 4 § första stycket Lirb, jfr med särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder i 4 kap. Lirb).

Om det i svensk rätt inte införs någon möjlighet till säkrande av uppgifter på annat snabbare och mindre ingripande sätt än exem-

pelvis genom hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation samt husrannsakan och beslag, innebär det att Sverige inte heller kan uppfylla konventionens krav på internationellt rättsligt samarbete.

Sammanfattningsvis gör vi alltså bedömningen att det krävs lagstiftning för att uppfylla konventionsåtagandet i denna del.

5.4.5 Skyndsamt säkrande och partiellt röjande av trafikuppgifter (artikel 17)

Bedömning: Det krävs lagstiftning för att uppfylla konventionens krav på skyndsamt säkrande och partiellt röjande av trafikuppgifter.

Skälen för bedömningen

I *artikel 17*, som har ett nära samband med artikel 16, finns speciella bestämmelser som gäller säkrande av trafikuppgifter.

Som framgått av redogörelsen över artikel 16 ska även trafikuppgifter kunna säkras. Enligt den förklarande rapporten (p. 166) kan det i en brottsutredning som gäller olika former av it-relaterad brottslighet inte sällan vara av avgörande betydelse för att kunna identifiera gärningsmännen att de brottsutredande myndigheterna får tillgång till trafikuppgifter. Just trafikuppgifter lagras emellertid enligt den förklarande rapporten ofta enbart under kort tid, varför det är viktigt att det finns möjlighet att sådana uppgifter i ett enskilt fall kan säkras för att eventuellt i ett senare skede lämnas ut. I många fall är flera leverantörer inblandade vid överföringen av ett meddelande. Det är därför inte säkert att det är tillräckligt att trafikuppgifter hos enbart en av leverantörerna i överföringskedjan säkras (se den förklarande rapporten p. 167). För att trafikuppgifter ska kunna säkras hos samtliga de leverantörer som deltagit vid överföringen krävs att dessa kan identifieras, vilket kan göras genom att den leverantör som först identifierats av de brottsutredande myndigheterna lämnar ut trafikuppgifter i den utsträckning som krävs för att fler leverantörer i överföringskedjan ska kunna identifieras (se den förklarande rapporten p. 169).

Enligt *punkt 1 a* ska en fördragsslutande stat se till att trafikuppgifter som avses i artikel 16 skyndsamt kan säkras, oavsett om en

eller flera tjänsteleverantörer har deltagit vid överföringen av meddelandet. Med begreppet *tjänsteleverantör* avses enligt artikel 1 c en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst.

Av *punkt 1 b* framgår att en fördragsslutande stat ska se till att en tillräcklig mängd trafikuppgifter skyndsamt röjs för statens behöriga myndighet, eller för en person utsedd av denna myndighet, för att tjänsteleverantörerna och den väg på vilken meddelandet överfördes ska kunna spåras.

Punkten 1 b går således längre än vad som följer av artikel 16, på så sätt att den innebär att vissa trafikuppgifter ska *lämnas ut*. Artikel 16 innebär, som framgått i avsnitt 5.4.4, enbart att bl.a. trafikuppgifter ska *säkras* för att i ett senare skede eventuellt lämnas ut. Det är emellertid i det tidiga utredningsskede som avses i artikel 17 fråga om ett mycket begränsat utlämnande av uppgifter där syftet enbart är att *identifiera övriga leverantörer* i överföringskedjan. Kraven gäller således inte ett uppgiftslämnande som avses i reglerna om hemlig övervakning av elektronisk kommunikation. De brottsutredande myndigheterna har att tydligt ange vilka uppgifter som behöver lämnas ut (se den förklarande rapporten p. 169).

I föregående avsnitt har redogjorts för de möjligheter som i svensk rätt för närvarande står till buds för brottsutredande myndigheter när det gäller att under en förundersökning säkra och även få tillgång till datorbehandlingsbara uppgifter. Vi har därvid dragit slutsatsen att det krävs lagstiftning för att uppfylla de krav som följer av artikel 16. Motsvarande bedömning görs även i fråga om kraven i artikel 17 på vissa uppgifter om sändningsvägar, eftersom det saknas regler om utlämnande av sådana uppgifter från en leverantör på annat sätt än genom hemlig övervakning av elektronisk kommunikation. Detta gäller även om uppgiftsutlämnandet enligt artikel 17 enbart syftar till att identifiera leverantörerna.

5.4.6 Skyldighet att lämna uppgifter (artikel 18)

Bedömning: Svensk rätt uppfyller konventionens krav på möjligheter att förelägga såväl enskilda att lämna ut särskilt angivna datorbehandlingsbara uppgifter som tjänsteleverantörer att lämna ut abonnentuppgifter.

Skälen för bedömningen

Artikel 18 innehåller bestämmelser om dels en allmän skyldighet för personer att lämna ut särskilt angivna datorbehandlingsbara uppgifter, dels en särskild skyldighet för tjänsteleverantörer att lämna ut abonnentuppgifter. Artikeln gäller enbart befintliga eller redan lagrade uppgifter.

Enligt *punkt 1 a* ska en fördragsslutande stat se till att det finns möjligheter för behöriga myndigheter att förelägga en person inom statens territorium att lämna ut särskilt angivna datorbehandlingsbara uppgifter som denne har i sin besittning eller under sin kontroll, och som lagras i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter. Med att en person har uppgifter i sin besittning avses att denne har uppgifterna i sin omedelbara fysiska besittning och med att en person har uppgifter under sin kontroll avses att personen, trots att uppgifterna finns lagrade någon annanstans, har rätt att bereda sig tillgång till dem (se den förklarande rapporten p. 173). Enbart det faktum att en person har teknisk möjlighet att få fram uppgifter innebär således inte att personen anses ha uppgifterna under sin kontroll.

Enligt *punkt 1 b* ska en tjänsteleverantör som erbjuder sina tjänster inom en fördragsslutande stats territorium kunna föreläggas att lämna ut abonnentuppgifter, oavsett om dessa finns lagrade i form av datorbehandlingsbara uppgifter eller i annan form, exempelvis på papper, som hänför sig till sådana tjänster och som tjänsteleverantören har i sin besittning eller under sin kontroll. Vad som i konventionens mening avses med begreppet tjänsteleverantör, se artikel 1 c och avsnitt 5.2.

Med *abonnentuppgifter* i artikelns mening avses enligt *punkt 3* 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 tillgängligt genom tjänsteavtalet eller tjänstearrangemanget, samt

c. övriga upplysningar om var kommunikationsutrustningen är belägen som är tillgängliga genom tjänsteavtalet eller tjänstearrangemanget.

Enligt den förklarande rapporten (p. 170) är artikelns syfte att det ska finnas utredningsåtgärder som gör det möjligt att få fram information av betydelse för brottsutredningar, som är mindre ingripande, störande och betungande för dem som innehar informationen än exempelvis husrannsakan och beslag och som därför ska utgöra alternativ till dessa tvångsåtgärder.

Eftersom artikel 15 som innehåller bestämmelser om rättssäkerhetsgarantier gäller även i förhållande till artikel 18, innebär det att det står en fördragsslutande stat fritt att ställa upp skilda former av villkor för att olika typer av uppgifter ska lämnas ut eller att uppgifter över huvud taget inte får lämnas ut när det gäller ringa brott (se den förklarande rapporten p. 174). En stat kan alltså exempelvis föreskriva att det krävs domstolsbeslut för att vissa uppgifter ska lämnas ut.

I den förklarande rapporten (p. 175) anges att de fördragsslutande staterna, trots att det inte uttryckligen nämns i artikeln, bör överväga att införa en möjlighet att ålägga den som ett föreläggande om utlämnande av uppgifter riktas mot att hemlighålla att åtgärden vidtagits.

För frågan om svensk rätt uppfyller kraven i punkt 1 a är främst reglerna om *beslag* och *edition* av betydelse.

Som framgått i avsnitt 5.4.4 kan brottsutredande myndigheter få tillgång till datorbehandlingsbara uppgifter genom beslag eftersom elektronisk information har en bärare som är att betrakta som ett föremål och därför kan tas i beslag. En förutsättning för beslag är att föremålet är tillgängligt när beslutet om åtgärden fattas. Beslagsrätten ger alltså inte någon befogenhet för beslutsfattaren att vidta åtgärder för att söka efter föremål. Som medel för att få fram föremålet kan exempelvis husrannsakan användas.

Editionsföreläggande innebär, som framgått i avsnitt 5.4.4, att den som innehar en skriftlig handling som kan antas ha betydelse som bevis är skyldig att förete den. Reglerna har i praxis ansetts tillämpliga även på elektroniskt lagrad information. Att den misstänkte och hans eller hennes närstående i brottmål är undantagna från editionsskyldighet är inte, mot bakgrund av bestämmelserna i artikel 15, något som står i konflikt med konventionsåtagandet. I artikel 15 hänvisas bl.a. till Europakonventionen och i kravet på rättvis rättegång enligt Europakonventionens artikel 6 anses ligga att den som är misstänkt för ett brott inte ska behöva bidra till utredningen eller bevisningen i målet, exempelvis genom att skaffa fram material som inte är till hans eller hennes fördel (”*the right not to incriminate oneself*”, se bl.a. Danelius, *Mänskliga rättigheter i europeisk praxis, En kommentar till Europakonventionen om de mänskliga rättigheterna*, 3:e uppl., s. 247–250).

Editionsföreläggande kan, liksom beslag, användas oberoende av brottets beskaffenhet. Åtgärden kan alltså användas vid förundersökning avseende samtliga de brott som föreläggandet att lämna ut särskilt angivna uppgifter enligt artikel 14.2 ska kunna tillämpas vid. Att ett editionsföreläggande kräver beslut av domstol är förenligt med konventionsåtagandet, eftersom något särskilt krav på skyndsamhet inte föreskrivs i artikel 18 (jfr det uttryckliga skyndsamhetskravet i artikel 16).

Editionsföreläggande kan inte användas innan någon är skäligen misstänkt för det brott förundersökningen avser. De åtgärder som avses i artikel 18 förefaller visserligen ha till syfte att kunna användas i ett tidigt skede av förundersökningen, men något hinder mot att uppställa krav på skälig misstanke för utlämnande av uppgifter finns inte, särskilt mot bakgrund av de rättssäkerhetsgarantier som kan och bör ställas upp enligt artikel 15.

Även om syftet med bestämmelserna i artikel 18 enligt den förklarande rapporten visserligen är att det ska finnas till husrannsakan och beslag alternativa och mindre ingripande åtgärder för att få fram information av betydelse för brottsutredningar, innebär konventionens reglering inte att det måste införas en sådan alternativ åtgärd i den nationella rätten. Konventionsbestämmelserna kan således uppfyllas genom exempelvis regler om beslag. I svensk rätt finns även, som framgått, möjlighet till editionsföreläggande.

Husrannsakan i förening med beslag och edition kan emellertid i svensk rätt inte användas för att få tillgång till elektronisk kommunikation hos en operatör. Mot den bakgrunden kan frågan ställas

hur artikel 18.1 a är att tolka när det gäller just uppgifter som finns hos en operatör.

Som nämnts har alltså i svensk rätt intagits den ståndpunkten att det inte bör komma i fråga att de brottsutredande myndigheterna använder editionsföreläggande eller husrannsakan i förening med beslag som substitut för tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation (se bl.a. prop. 2002/03:74 s. 45–46).

Uppgifter om meddelanden hos en operatör kan därför inte hämtas in med stöd av beslag och editionsföreläggande. När det gäller uppgifter om meddelanden som kan finnas både hos den enskilde och hos operatören kan de brottsutredande myndigheterna antingen använda sig av reglerna om hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation eller använda andra tvångsmedel, t.ex. husrannsakan och beslag hos den enskilde (se bl.a. SOU 1998:46 s. 373). Som framgått, gäller i hög utsträckning olika villkor för användningen av hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation å ena sidan och tvångsmedlen husrannsakan och beslag samt edition å den andra. Information om meddelanden i ett elektroniskt kommunikationsnät åtnjuter alltså olika grad av skydd beroende på var uppgifterna om meddelandet finns.

I övrigt gäller att historiska uppgifter som finns lagrade hos en operatör är möjliga att få ut i svensk rätt genom bestämmelserna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Det bör vidare framhållas att punkt 1 a avser utlämnande av historiska uppgifter som redan finns lagrade. Inte sällan torde sådant utlämnande från en operatör gälla trafikuppgifter. Sådana uppgifter kan de brottsbekämpande myndigheterna få tillgång till genom hemlig övervakning av elektronisk kommunikation. För detta tvångsmedel gäller lägre krav på brottets svårhetsgrad än för hemlig avlyssning av elektronisk kommunikation. Hemlig övervakning av elektronisk kommunikation får användas när förundersökningen avser ett brott för vilket det inte är föreskrivet lindrigare straff än sex månaders fängelse eller dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling eller försök, förberedelse eller stämpling till sådant brott om gärningen är belagd med straff. Tvångsmedlet kan mot den bakgrunden i relativt hög utsträckning användas i förundersökningar avseende sådana gärningar som konventionen avser att straffbelägga och även vid andra typer av brott då brottet begåtts med hjälp av

ett datorsystem, om brottet är av visst allvar. Mot bakgrund av artikel 15 står det, som nämnts, en fördragsslutande stat fritt att i viss utsträckning ställa upp skilda former av villkor för att olika typer av uppgifter ska lämnas ut.

Sammanfattningsvis är det vår uppfattning att den svenska regleringen av de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation hos en operatör är förenlig med regleringen i punkt 1 a. Det är vidare vår uppfattning att svensk rätt genom främst bestämmelserna om beslag och edition måste anses uppfylla kraven enligt punkt 1 a.

För frågan om svensk rätt uppfyller kraven i *punkt 1 b* är bestämmelser i 6 kap. LEK av betydelse.

Enligt 6 kap. 22 § första stycket 2 LEK ska den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift om abonnemang i samband med misstanke om brott på begäran lämna ut uppgiften till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet. Sedan den 1 juli 2012 är skyldigheten att lämna ut abonnemangsuppgifter inte begränsad till brott av viss svårhet (prop. 2011/12:55 s. 102–103). Som framgår av bestämmelsen gäller skyldigheten att lämna ut uppgifter om abonnemang ”den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst”. Skyldigheten gäller därmed alla leverantörer. Det krävs inte att det nät eller den tjänst som leverantören tillhandahåller är allmänt/allmän (se Post- och telestyrelsens [PTS] ”*Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter*”, 2006-11-28 och SOU 2009:1 s. 69–70). Även en leverantör som inte är anmälningspliktig enligt 2 kap. 1 § LEK omfattas således av skyldigheten att lämna ut uppgifter om abonnemang. Kretsen av leverantörer som omfattas av konventionens definition av tjänsteleverantör, är således inte vidare än den krets som omfattas av skyldigheten att lämna ut uppgift om abonnemang enligt 6 kap. 22 § första stycket 2 LEK.

I 6 kap. 21 § första stycket 5 LEK finns en straffsanktionerad tystnadsplikt för leverantörerna när det gäller uppgifter som gäller myndigheters inhämtning av uppgift om abonnemang i syfte att utreda brott.

Med uppgifter om abonnemang avses i den svenska lagstiftningen främst uppgifter om namn, titel adress och abonnentnummer. Sådana uppgifter kallas ibland kataloguppgifter (prop. 2011/12:55 s. 100). Även s.k. dynamiska IP-nummer, vilka är unika nummer som kan

användas för att identifiera en abonnent som är uppkopplad mot internet, är att betrakta som en uppgift om abonnemang (prop. 2011/12:55 s. 101).

Uppgifter om vilka som har deltagit i utväxlingen av ett elektroniskt meddelande samt när och under hur lång tid utväxlingen ägde rum, liksom uppgifter om positionen hos en mobiltelefon anses i svensk rätt vara att hänföra till kategorin ”uppgift som angår ett särskilt elektroniskt meddelande” (6 kap. 20 § första stycket 3 LEK, prop. 2011/12:55 s. 100). I förundersökningar får sådana uppgifter inhämtas från operatörer enbart efter beslut om hemlig övervakning av elektronisk kommunikation eller hemlig avlyssning av elektronisk kommunikation.

Konventionens definition av abonnentuppgifter i artikel 18 kan förefalla skilja sig från vad som i svensk rätt avses med uppgifter om abonnemang. Som framgått (se punkt 3), anges emellertid att som abonnentuppgifter i artikelns mening aldrig ska anses sådana uppgifter som är trafikuppgifter eller innehållsuppgifter. Med hänsyn till denna begränsningsgrund gör vi bedömningen att konventionens definition av abonnentuppgifter och det som i svensk rätt avses med uppgifter om abonnemang i huvudsak sammanfaller. Såväl enligt konventionen som i svensk rätt är det alltså fråga om sådana uppgifter som kan anses som identitetsuppgifter.

Mot bakgrund av det anförda är det vår uppfattning att den skyldighet som enligt 6 kap. 22 § första stycket 2 LEK finns för leverantörer att till brottsbekämpande myndigheter, oavsett brottets svårhetsgrad, lämna ut uppgifter om abonnemang innebär att svensk rätt uppfyller kraven enligt punkt 1 b. Som framgått gäller även tystnadsplikt för leverantörerna när det gäller uppgifter som gäller myndigheters inhämtning av uppgift om abonnemang i syfte att utreda brott.

5.4.7 Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter (artikel 19)

Bedömning: De svenska bestämmelserna om husrannsakan uppfyller konventionens krav på möjlighet att genom husrannsakan eller på liknande sätt bereda sig tillgång till datorsystem och lagrade datorbehandlingsbara uppgifter samt medium för lagring av datorbehandlingsbara uppgifter. Dessa bestämmelser uppfyller

vidare konventionens krav på möjlighet att skyndsamt utvidga en husrannsakan till att avse andra datorsystem.

De svenska beslagsreglerna uppfyller konventionens krav på säkrande av datorbehandlingsbara uppgifter som har påträffats genom husrannsakan, såväl vad gäller säkrande av datorsystem, kopiering av datorbehandlingsbara uppgifter, bevarande av lagrade datorbehandlingsbara uppgifters integritet som möjligheten att göra datorbehandlingsbara uppgifter oåtkomliga.

De svenska reglerna om vittnesförhör inför rätta under en förundersökning uppfyller formellt sett konventionens krav på möjlighet att förelägga en person med kunskap om ett datorsystems funktion eller om åtgärder som tillämpas för att skydda datorbehandlingsbara uppgifter, att lämna information som är nödvändig för att möjliggöra husrannsakan. Det finns dock skäl att överväga att i svensk rätt införa en specifik möjlighet till föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö.

Skälen för bedömningen

Artikel 19 innehåller bestämmelser om husrannsakan och beslag av datorbehandlingsbara uppgifter.

Enligt *punkt 1* ska myndigheter i en fördragsslutande stat ha rätt att genom *husrannsakan eller på liknande sätt* bereda sig tillgång till ett datorsystem, en del därav eller ett annat medium för lagring av datorbehandlingsbara uppgifter och de uppgifter som finns lagrade däri.

Av *punkt 2* framgår att myndigheterna, när de genom husrannsakan eller på liknande sätt bereder sig tillgång till ett visst datorsystem eller en del därav 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 ska kunna *utvidga* husrannsakan eller den liknande åtgärden till att bereda sig åtkomst till det andra systemet.

Enligt *punkt 3* ska myndigheterna ha rätt att *beslagta* eller på liknande sätt *säkra* datorbehandlingsbara uppgifter som har åtkommits enligt punkterna 1 och 2. Myndigheterna ska därvid ha 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 uppgifterna,

c. bevara uppgifternas *integritet*, och

d. göra uppgifterna *oåtkomliga* eller *avlägsna* dem från det datorsystem till vilket åtkomst har beretts.

Av *punkt 4* följer att myndigheterna ska ha möjlighet 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 husrannsakan enligt punkterna 1 och 2.

Av den förklarande rapporten (p. 184) framgår att syftet med artikeln är att modernisera regler om husrannsakan och beslag så att det i de fördragsslutande staternas nationella lagstiftning finns bestämmelser som gör det möjligt att genom husrannsakan och beslag säkra lagrade datorbehandlingsbara uppgifter på samma sätt som går att göra när det gäller materiella saker. De nationella lagföreskrifterna om användning av husrannsakan och beslag är inte avsedda att påverkas på annat sätt än att göra dem tillämpliga på elektroniska uppgifter.

I svensk rätt finns bestämmelser om *husrannsakan* i brottsutredande syfte i 28 kap. rättegångsbalken.

Husrannsakan kan vara reell eller personell, dvs. avse antingen föremål eller personer. I detta sammanhang är endast reell husrannsakan av betydelse. Reell husrannsakan får enligt 28 kap. 1 § rättegångsbalken företas i hus, rum eller annat slutet förvaringsställe för att söka efter föremål som kan tas i beslag eller i förvar eller annars för att utröna omständigheter som kan vara av betydelse för utredning om brottet eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken. För sådan husrannsakan fordras att det finns anledning att anta att ett brott har begåtts på vilket fängelse kan följa.

Husrannsakan innefattar alltså en undersökning av hus, rum eller annat slutet förvaringsställe. Med hus avses inte bara bostadshus utan även andra byggnader, såsom ekonomi- och uthusbyggnader samt fabriker och magasin. Begreppet rum omfattar förutom bo-

stadsrum även kontors- och lagerlokaler och till slutet förvaringsställe räknas t.ex. en stängd bil (SOU 1938:44 s. 328). 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.

Hos annan än den som skäligen kan misstänkas för brottet får husrannsakan företas i tre särskilda fall, nämligen om brottet har begåtts hos honom eller henne, den misstänkte har gripits där eller om det annars finns synnerlig anledning att det vid genomsökningen ska anträffas föremål som kan tas i beslag eller i förvar eller att annan utredning om brottet eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken kan vinnas.

För husrannsakan hos den misstänkte får inte i något fall åberopas hans eller hennes samtycke, om inte den misstänkte själv har begärt att åtgärden ska vidtas.

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 rättegångsbalken). Med lokal som är tillgänglig för allmänheten avses bl.a. butiker, restauranger, kaféer, teater- och biograflokaler. Ett internetcafé som är öppet för allmänheten kan alltså 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 rättegångsbalken). 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 (28 kap. 3 § tredje stycket rättegångsbalken).

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

Eftersom syftet med husrannsakan normalt är att söka efter föremål som kan tas i beslag innebär det att om beslag är uteslutet, exempelvis på grund av reglerna om beslagsförbud i 27 kap. 2 § rättegångsbalken (se närmare i det följande), får husrannsakan inte

göras för att söka efter föremålet eller handlingen (Fitger, *Rättegångsbalken I*, s. 28:4 b).

Förordnande om sådan husrannsakan som här avses meddelas av undersökningsledaren, åklagaren eller rätten (28 kap. 4 § första stycket rättegångsbalken). Om husrannsakan kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den hos vilken åtgärden vidtas bör emellertid rätten, om det inte är fara i dröjsmål, besluta om åtgärden. Vid fara i dröjsmål får polisman enligt 28 kap. 5 § rättegångsbalken företa husrannsakan även utan beslut från behörig befattningshavare.

Enligt 28 kap. 9 § rättegångsbalken ska det föras protokoll över husrannsakan där bl.a. ändamålet med åtgärden ska anges.

Befogenheten för de brottsutredande myndigheterna att vid en husrannsakan söka efter uppgifter som finns lagrade i datorer är inte närmare reglerad. Det finns alltså inte några särregler om undersökning av datorer. Det är inte heller ovanligt att polisen bereder sig tillgång till datorer för att inhämta uppgifter i brottsutredande syfte. Polisen anses berättigad att under en husrannsakan söka efter information i en dator lika väl som att läsa de handlingar eller studera andra föremål som påträffas under en husrannsakan (prop. 1998/99:11 s. 41, se också SOU 1995:47 s. 184). Under en husrannsakan kan därför datorer som finns i lokalen undersökas för att finna elektroniska dokument, filer eller spår av kommunikation.

Som nämnts i avsnitt 5.4.4 får hos en operatör uppgifter om meddelanden i ett elektroniskt kommunikationsnät inte hämtas in med stöd av husrannsakan. Åtkomsten till sådana uppgifter regleras i stället exklusivt genom bestämmelserna i rättegångsbalken om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation samt till viss del, när det gäller abonnentuppgifter, genom bestämmelser i LEK.

Då en lokal genomsöks efter beslut om husrannsakan kan alltså även en dator eller annan teknisk utrustning som finns i lokalen undersökas i syfte att bl.a. få klarhet i om det finns grund för beslag. Något särskilt beslut för att undersöka datorn behövs då inte. Normalt finns datorer, även bärbara datorer, i lokaler till vilka brottsutredande myndigheter inte har tillträde utan beslut om husrannsakan. I praktiken är det därför sällan aktuellt att ta ställning till om ett särskilt beslut om husrannsakan av själva datorn kan fattas (se Lindberg, *Straffprocessuella tvångsmedel*, tredje upplagan, 2012, s. 584, jfr andra upplagan, 2009, s. 562).

Mot den angivna bakgrunden är det vår uppfattning att svensk rätt genom bestämmelserna om husrannsakan uppfyller de krav som uppställs i artikel 19.1. Husrannsakan kan användas vid samtliga brott som anges i artikel 14.2. De begränsningar för husrannsakan som svensk rätt uppställer när det gäller bl.a. proportionalitet och kopplingen till reglerna om beslagsförbud, är godtagbara mot bakgrund av bestämmelserna i artikel 15.

När det gäller regleringen i artikel 19.2 och möjligheten att skyndsamt utvidga husrannsakan till ett annat datorsystem än det som undersökts med stöd av det ursprungliga beslutet om husrannsakan, kan följande sägas. Det torde för närvarande i svensk rätt vara osäkert om det är tillåtet att inom ramen för en husrannsakan i en lokal vid vilken en dator som finns i lokalen undersöks, genom den datorn bereda sig tillgång till information som finns lagrad i en annan dator eller datorsystem. Artikel 19.2 ställer emellertid enbart krav på att det ska vara möjligt att skyndsamt utvidga undersökningen av ett datorsystem till att omfatta ett annat datorsystem inom den fördragsslutande statens territorium, om de brottsutredande myndigheterna vid undersökningen av det första datorsystemet har anledning att tro att de uppgifter som eftersöks är lagrade i det andra systemet. Det är inte närmare reglerat hur en sådan utvidgad undersökning ska gå till. Varje fördragsslutande stat får alltså själv välja vilka villkor som ska gälla för den utvidgade undersökningen. I den förklarande rapporten (p. 194) anges att konventionens krav i denna del kan uppfyllas exempelvis genom att husrannsakan genomförs i en samordnad och snabb aktion såväl på platsen för det första datorsystemet som för det andra. En sådan typ av utvidgad undersökning av ett tillkommande datorsystem kan redan i dag göras med stöd av de svenska reglerna om husrannsakan. I de flesta fall kan husrannsakan ske utan förordnande av rätten. Det finns därför förutsättningar för åklagare eller annan undersökningsledare att, på det sätt som konventionsartikeln förutsätter, skyndsamt fatta ett beslut om husrannsakan av platsen för det andra datorsystemet och se till att det verkställs med hjälp av polis som finns där. Det bör noteras att konventionen anger att det ska vara fråga om husrannsakan *inom* den fördragsslutande statens territorium.

Vår bedömning är att svensk rätt redan i dag uppfyller de krav som uppställs i artikel 19.2 avseende möjligheterna att skyndsamt utvidga en husrannsakan till att avse ett tillkommande datorsystem. Några lagstiftningsåtgärder krävs därför inte.

När det gäller *beslag* av datorbehandlingsbara uppgifter har de svenska beslagsreglerna redovisats i avsnitt 5.4.4. Som framgår i det avsnittet kan datorbehandlingsbara uppgifter säkras genom beslag trots att de svenska beslagsreglerna utgår från att det som kan tas i beslag är lösa saker, eftersom elektronisk information har en bärare, exempelvis en dator, en mobiltelefon eller ett fickminne, som är att betrakta som ett föremål och därför kan tas i beslag. I sammanhanget bör nämnas att Förundersökningsutredningen, som analyserat reglerna om beslag i it-miljö, nyligen konstaterat att beslagsreglerna visat sig fungera tillfredsställande när det gäller möjligheten att ta elektroniska uppgifter i beslag (SOU 2011:45 s. 353). De problem som uppmärksammats i sammanhanget var i stället, enligt Förundersökningsutredningen, knutna till reglerna om beslagsförbud (se närmare nedan).

Beslag får enligt 27 kap. 1 § första stycket rättegångsbalken göras i fyra olika syften. För det första får föremål som skäligen kan antas ha betydelse för utredning om brott tas i beslag (bevisbeslag). Beslag får också företas för att återställa egendom som någon avhänts genom brott (återställandebeslag). Vidare får beslag göras i syfte att säkerställa förverkande av föremål på grund av brott (förverkandebeslag). Slutligen får beslag göras av föremål som kan antas ha betydelse för utredning om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken.

Reglerna om beslag av föremål är tillämpliga även på skriftliga handlingar om inte annat är föreskrivet. Vad som avses med skriftlig handling är inte definierat i rättegångsbalken. I 27 kap. 2 § finns förbud mot beslag av vissa skriftliga handlingar. Bestämmelsen anknyter till reglerna i 36 kap. 3 och 5 §§ rättegångsbalken om undantag från vittnesplikten. Handlingar som kan antas innehålla uppgifter som ett vittne med stöd av 36 kap. 5 § rättegångsbalken kan vägra uttala sig om får inte tas i beslag och inte heller får skriftliga meddelanden mellan den misstänkte och närstående till denne och mellan sådana närstående inbördes tas i beslag. Beslagsförbudet i det senare fallet gäller inte om brottet är så allvarligt att det lägsta föreskrivna straffet är fängelse i två år.

Enligt sin ordalydelse gäller alltså beslagsförbudet endast skriftliga handlingar och meddelanden. Det har framförts olika uppfattningar i fråga om regelns räckvidd vad gäller elektroniska handlingar. Vissa har hävdat att bestämmelserna kan tillämpas analogt på sådana, medan andra haft motsatt uppfattning (se SOU 2011:45 s. 291–296). Rättsläget är alltså oklart i denna fråga. Förundersöknings-

utredningen, som bl.a. hade i uppdrag att dels göra en översyn av hur reglerna om beslagsförbud för vissa skriftliga handlingar tillämpas på elektroniska uppgifter och handlingar, dels överväga om det i syfte att stärka skyddet för information som lagras i elektronisk form fanns anledning att komplettera dessa regler, anförde i sitt slutbetänkande *Förundersökning – objektivitet, beslag, dokumentation m.m.* (SOU 2011:45 s. 352–353) att ovissheten om vad som gäller i detta avseende är otillfredsställande, eftersom den kan innebära att uppgifter som är avsedda att omfattas av beslagsförbudet åtnjuter ett sämre skydd om de finns upptagna i elektronisk form än om de finns i en skriftlig handling. Enligt Förundersökningsutredningens mening borde därför skyddet för elektroniskt lagrad information – som skulle ha omfattats av beslagsförbudet om den framgått av en skriftlig handling – stärkas.

Som framgått, anses datorer och andra informationsbärare enligt gällande rätt få genomsökas inom ramen för en husrannsakan. I praktiken torde det dock vara sällsynt att det sker en sådan genomgång, eftersom det vanligtvis finns en mycket stor informationsmängd lagrad i en dator. Det normala förfarandet är i stället att informationsbäraren som ett första steg tas i beslag för att därefter genomsökas. En ordning som förutsätter att de brottsutredande myndigheterna genomsökte innehållet i exempelvis en dator före ett eventuellt beslut om beslag skulle kräva omfattande resurser. Information i en dator är inte omedelbart tillgänglig på samma sätt som pappersdokument. Mot den bakgrunden gjorde Förundersökningsutredningen bedömningen att bestämmelserna om beslagsförbud inte bör göras direkt tillämpliga på elektroniska handlingar eller uppgifter (SOU 2011:45 s. 354). Utredningen föreslog i stället att det ska uppställas särskilda regler för hur genomsökningen av beslagtagna datorer och andra informationsbärare ska gå till, om det i det enskilda fallet finns omständigheter som talar för att exempelvis en dator innehåller skyddsvärda uppgifter (SOU 2011:45 s. 355–360).

Enligt Förundersökningsutredningens förslag ska därför om en digital informationsbärare som tas i beslag kan antas innehålla uppgifter för vilka beslagsförbud gäller, bl.a. den hos vilken beslaget gjorts beredas tillfälle att närvara vid genomsökningen av informationsbäraren. En sådan närvarorätt ska enligt förslaget inte gälla för uppgifter mellan närstående. Om det vid en genomsökning av en digital informationsbärare visar sig att innehållet omfattas av beslagsförbud, får vidare enligt förslaget den befattningshavare som utför genomsökningen inte ta ytterligare del av detta innehåll.

Förundersökningsutredningens förslag bereds för närvarande i Regeringskansliet.

Om Förundersökningsutredningens förslag i den nu aktuella delen genomförs, innebär det att rättsläget i fråga om beslagsförbudsreglernas räckvidd vad gäller elektroniska handlingar klargörs. Enligt vår bedömning uppfyller emellertid nuvarande svenska regler om beslag konventionens krav på möjlighet att beslagta datorbehandlingsbara uppgifter enligt artikel 19.3 a. Huruvida Förundersökningsutredningens förslag i denna del leder till lagstiftning eller inte, eller om de föreslagna lagändringarna ännu inte skulle ha hunnit träda i kraft vid tidpunkten för en svensk ratifikation av konventionen, saknar därför betydelse för frågan om svensk rätts förenlighet med konventionen. Mot bakgrund av artiklarna 14 och 15, och kraven på rättssäkerhetsgarantier, möter det inte något hinder att i svensk rätt ha regler som innebär förbud mot beslag i de situationer som beslagsförbudsreglerna tar sikte på, eller att införa sådana speciella regler för hur genomsökningen av beslagtagna datorer och andra informationsbärare ska gå till som Förundersökningsutredningen har föreslagit. Någon lagstiftning för att uppfylla kraven i artikel 19.3 a krävs alltså inte.

Artikel 19.3 b innebär, som framgått, att det ska finnas möjlighet att framställa och behålla en kopia av datorbehandlingsbara uppgifter som åtkommits genom husrannsakan eller på liknande sätt.

Det är mycket vanligt att brottsutredande myndigheter i Sverige av olika skäl kopierar beslagtaget material, både fysiska skriftliga handlingar och elektronisk information som lagrats i t.ex. datorer. Förfarandet är oreglerat, men frågan om kopiering har behandlats i flera offentliga utredningar och rättsfall samt har berörts av JK och JO (se närmare SOU 2011:45 s. 332).

Högsta domstolen har slagit fast att kopior inte utgör beslagtagen egendom (se bl.a. NJA 1988 s. 471). Detta innebär att beslagsreglerna i t.ex. 27 kap. rättegångsbalken inte är tillämpliga på kopierat material som finns kvar när ett beslag hävts, vilket i sin tur innebär att, om ett beslag kopieras och därefter hävs, den som drabbats av åtgärden i princip inte har någon möjlighet att få beslagsbeslutets giltighet prövat av rätten, eftersom saken förfallit i och med upphävandet av beslaget. Avsaknaden av reglering innebär också att det är osäkert hur kopiorna ska hanteras när de inte längre behövs.

Förundersökningsutredningen hade mot denna bakgrund till uppgift att överväga även om kopiering av beslagtaget material borde lagregleras. Utredningen konstaterade därvid inledningsvis

att de invändningar som riktats mot förfarandet att kopiera material i första hand inte rörde själva *förfaringssättet* att kopiera material som tagits i beslag, utan snarare *bristen på regler* som styr hanteringen av kopiorna när beslaget väl upphört (SOU 2011:45 s. 332). Utredningen konstaterade vidare att kopiering av beslagtaget material ofta kan ligga i den enskildes intresse eftersom, om kopiering tillåts ske, han eller hon nämligen mycket snabbare kan få tillbaka det som tagits i beslag varvid intrånget minskar, och att kopieringsförfarandet, speciellt när det gäller beslag i it-miljö, innebär många fördelar i effektivitets-, utrednings- och rättssäkerhetshänseende (s. 334). Enligt Förundersökningsutredningens mening talade därför de fördelar som kopiering innebär med styrka för att förfarandet generellt sett måste vara tillåtet. Utredningen slog även fast att det inte heller torde råda några delade meningar om detta (s. 334).

Utredningens bedömningar och förslag (s. 334–352) mynnade i huvudsak ut i att

- det ska framgå av lag att kopiering av beslagtagen egendom får ske,
- det inte bör uppställas några särskilda förutsättningar för att beslag ska få kopieras,
- det inte är lämpligt att i författning införa begränsningar av de olika tekniska metoder som kan användas i samband med kopiering av beslagtaget material,
- det inte bör införas någon möjlighet till domstolsprövning av beslag som har hävts, samt att
- det inte bör införas några särskilda bestämmelser om gallring av kopior utan dessa bör bevaras på samma sätt som utredningsmaterial i övrigt.

Förundersökningsutredningens förslag till lagstiftning om kopiering innebär i princip endast en kodifiering av den praxis som råder, dvs. att kopiering får användas när det finns skäl för det. Syftet med förslagen är att utrymmet för de brottsutredande myndigheterna att kopiera beslagtaget material även fortsättningsvis ska vara stort (s. 337).

När det gäller kopiering av datalagrad information finns två olika metoder som används när information ska säkras vid beslag i it-miljö (se närmare SOU 2011:45 s. 281–283 och 338). En metod är s.k. *spegling* eller *spegelkopiering*. Metoden innebär att en kopia av

allt innehåll i en hårddisk skapas och förs över på ett annat lagringsmedium. Den speglade kopian utvisar därmed den ursprungliga hårddiskens exakta innehåll vid tidpunkten för åtgärden. Kopian är inte möjlig att ändra eller manipulera. Spegling sker med hjälp av en särskild programvara och kan verkställas antingen på platsen där beslaget görs eller i polisens lokaler. I det sistnämnda fallet förutsätts att ett formellt beslag av utrustning sker. Även om spegling sker på plats bör åtgärden av rättssäkerhetsskäl föregås av ett beslag (SOU 2011:45 s. 281).

En annan teknik som kan användas är att genom *selektiv kopiering* framställa kopior av vissa specifika dokument eller filer och sedan föra över dessa till t.ex. en CD eller ett USB-minne. Metoden förutsätter att den som verkställer åtgärden vet vad som eftersöks.

Skillnaden mellan spegling och selektiv kopiering består väsentligen i att all information i hårddisken kan tas tillvara när speglingstekniken används. Genom speglingen blir även borttagna filer som inte hunnit skrivas över samt rester av delvis överskrivna filer tillgängliga för analys. Sådan information, som kan vara av stort intresse i en brottsutredning, kan inte säkras och återskapas genom den selektiva kopieringsmetoden. Den omständigheten att den speglade kopian inte kan förändras innebär också att invändningar om att de brottsutredande myndigheterna manipulerat innehållet lättare kan utredas.

Speglingstekniken har också nackdelar. Eftersom kopian inte kan ändras är det inte heller möjligt att skilja ut och ta bort delar av materialet som inte längre behövs i brottsutredningen. Detsamma gäller sådan information som kan omfattas av beslagsförbudet enligt 27 kap. 2 § RB. Speglingstekniken skapar också stora mängder överskottsinformation.

Speglingstekniken har alltså ett antal fördelar, men inger också vissa tveksamheter ur integritetssynpunkt. Förundersökningsutredningen övervägde därför om det fanns anledning att införa någon form av begränsning av teknikens användningsområde. Enligt utredningens uppfattning var dock en sådan gränsdragning svår att göra i praktiken, bl.a. eftersom en begränsningsbestämmelse mot bakgrund av den snabba tekniska utvecklingen snabbt skulle riskera att bli överspelad eller kräva justeringar (SOU 2011:45 s. 339). Utredningen gjorde därför den bedömningen att det inte var lämpligt att i författning införa begränsningar av de olika tekniska metoder som kan användas i samband med kopiering av beslagtaget material och att användningen av exempelvis speglingsmetoden, i enlighet

med nuvarande reglering, får begränsas med hjälp av proportionalitetsprincipen (SOU 2011:45 s. 339).

Som framgått av det anförda används såväl spegelkopiering som selektiv kopiering redan i dag i stor utsträckning av de brottsbekämpande myndigheterna. Den härskande uppfattningen är också att kopiering av beslagtaget material måste vara tillåtet. Några egentliga invändningar mot att förfarandet, trots avsaknad av uttryckligt författningsstöd, tillämpas redan i dag finns alltså inte. Även om Förundersökningsutredningens förslag i denna del inte skulle leda till lagstiftning, eller förslagen ännu inte ha trätt i kraft vid en svensk ratificering av konventionen, får dock anses att svensk rätt uppfyller konventionens krav i artikel 19.3 b.

Den möjlighet att *behålla* en kopia av de datorbehandlingsbara uppgifterna som föreskrivs i artikel 19.3 b innebär, enligt vår mening, att de kopierade uppgifterna ska finnas tillgängliga för de brottsutredande myndigheterna under den tid som brottsutredningen pågår. Någon skyldighet att behålla de kopierade uppgifterna även efter att en förundersökning avslutats, föreskrivs alltså inte i artikeln (jfr motsvarande bedömning av Förundersökningsutredningen, SOU 2011:45 s. 342). Svensk rätt lever redan upp till artikelns krav i detta avseende.

Sammanfattningsvis är det således vår uppfattning att svensk rätt, oberoende av om Förundersökningsutredningens förslag i fråga om kopiering av beslagtagen egendom genomförs, uppfyller konventionskravet i artikel 19.3 b.

Enligt artikel 19.3 c ska de lagrade datorbehandlingsbara uppgifternas integritet bevaras, med vilket avses att de uppgifter som tas i beslag eller kopieras ska vara under de brottsutredande myndigheters kontroll så att uppgifterna inte kan förändras under den tid som brottsutredningen eller brottmålsförfarandet pågår (se den förklarande rapporten p. 197). De svenska reglerna om beslag och möjligheten till kopiering (genom spegling eller annan form av kopiering) innebär att svensk rätt uppfyller konventionens krav i denna del.

Enligt artikel 19.3 d ska det vara möjligt att göra de datorbehandlingsbara uppgifter som påträffats vid exempelvis en husrannsakan oåtkomliga eller avlägsna dem från det datorsystem till vilken åtkomst har beretts. Punkten 3 d måste läsas i det sammanhang där den förekommer. Samtliga de åtgärder som räknas upp i punkten 3 har till syfte att under en brottsutredning säkra datorbehandlingsbara uppgifter och se till att dessa behålls intakta under utredningens

gång. Ett ytterligare syfte med punkten 3 d är att förhindra att uppgifterna används för att orsaka skada, exempelvis om det är fråga om virusprogram eller instruktioner om tillverkning av virus eller sprängmedel, eller om innehållet i uppgifterna är olagligt, exempelvis om det är fråga om barnpornografi. Säkrandet av uppgifter enligt konventionen har alltså två syften: dels att säkra bevis, dels att konfiskera uppgifter. Att göra uppgifterna oåtkomliga eller avlägsna dem från ett visst datorsystem ska alltså inte läsas som att uppgifterna slutligt ska förstöras eller raderas. Den misstänkte ska tillfälligt vara fråntagen uppgifterna men han eller hon ska eventuellt kunna få tillgång till dem igen efter avslutad brottsutredning eller process. Användning av uppgifter kan förhindras exempelvis genom kryptering eller på annat lämpligt sätt (se den förklarande rapporten p. 198 och 199).

Enligt 27 kap. 10 § första stycket rättegångsbalken ska ett beslagtaget föremål som huvudregel tas i förvar av den som verkställt beslaget. Föremålet får dock lämnas kvar i innehavarens besittning, under förutsättning av att det kan ske utan fara och även i övrigt är lämpligt. Ett föremål som lämnas kvar i innehavarens besittning ska förseglas eller märkas som beslagtaget, om detta inte framstår som obehövligt.

Beslag i svensk rätt innebär alltså att en brottsutredande myndighet tillfälligt tar hand om annans egendom och att den som äger föremålet inte har möjlighet att fritt disponera detta (se Lindberg, *Straffprocessuella tvångsmedel*, tredje upplagan, 2012, s. 383). Som tidigare angetts får beslag göras såväl i syfte att utreda brott som i syfte att säkerställa förverkande av föremål på grund av brott.

Som framgått, kan konventionskravet i artikel 19.3 d om förhindrande av användningen av de uppgifter som där avses uppfyllas på lämpligt sätt och i nationell rätt behöver exempelvis inte införas möjlighet för brottsutredande myndigheter att begränsa åtkomst till uppgifter genom kryptering. Vår uppfattning är att de svenska beslagsreglerna uppfyller konventionens krav på möjlighet att göra datorbehandlingsbara uppgifter som åtkommits vid exempelvis en husrannsakan oåtkomliga.

Enligt artikel 19.4 ska det, som framgått, vara möjligt att förelägga en person som har kännedom om ett datorsystem, eller om säkerheten kring detta, att – i den mån det är skäligt – lämna information som är nödvändig för att möjliggöra husrannsakan enligt punkterna 1 och 2 i artikeln.

I svensk rätt är alla som kan antas ha upplysningar av betydelse för utredningen, enligt 23 kap. 6 § rättegångsbalken, skyldiga att underkasta sig förhör under en förundersökning. Någon skyldighet för den som hörs (vittnen, målsägande eller misstänkt) att uttala sig under förhöret finns dock inte. Den som uttalar sig har inte heller någon skyldighet att tala sanning. Bestämmelsen i 23 kap. 6 § rättegångsbalken innebär alltså inte att någon kan föreläggas att lämna information på det sätt som artikel 19.4 förutsätter.

Under en förundersökning kan emellertid, enligt 23 kap. 13 § rättegångsbalken, förundersökningsledaren kräva att det hålls vittnesförhör inför rätta. Samma skyldighet för ett vittne att uttala sig gäller då som vid ett vanligt vittnesförhör. Ett sådant förhör förutsätter emellertid antingen att den som ska höras har vägrat yttra sig om en omständighet som är av vikt för utredningen eller att det annars är av synnerlig vikt för utredningen att han eller hon hörs som vittne redan under utredningen. Ytterligare en förutsättning är att det finns någon som är skäligen misstänkt. Den misstänkte ska också ges tillfälle att närvara vid förhöret. Möjligheten till förhör inför rätta under förundersökningen gäller enbart vittnen och inte målsäganden eller misstänkta.

I promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att några nya regler i svensk rätt som ålägger en person med särskild kunskap om ett visst datorsystem att lämna information som underlättar verkställandet av tvångsmedel, inte krävdes för att uppfylla åtagandet i artikel 19.4 (Ds 2005:6 s. 328–330). Enligt promemorian torde i de fall där ett intrång har ägt rum utan medverkan av ägaren eller brukaren av ett datorsystem denne i eget intresse bidra med alla de upplysningar som kan behövas för att underlätta verkställigheten av tvångsåtgärder. Det kunde därför, anfördes det, 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. Något behov av ytterligare regler som tar sikte på målsägande behövdes därför inte, anfördes det i promemorian. Ett föreläggande mot någon som är misstänkt kan, enligt uppfattningen i promemorian, mot bakgrund av artikel 6 i Europakonventionen och förbudet mot *self-incrimination* i FN:s konvention om medborgerliga och politiska rättigheter, inte godtas. När det gäller vittnen fick de regler om vittnesförhör inför rätta som nyss redogjorts för, enligt uppfattningen i promemorian, anses

utgöra en tillräcklig garanti för att få fram de uppgifter som krävs av en helt utomstående.

Vi delar uppfattningen att ett föreläggande mot någon som är misstänkt, av de i promemorian nämnda skälen, inte kan accepteras. Det kan inte heller vara avsikten att artikel 19.4 ska tolkas på det sättet att ett föreläggande ska kunna riktas mot en misstänkt (jfr artikel 15).

Det är inte självklart att det kan förutsättas att en målsägande i alla lägen är villig att självmant bidra med information som underlättar husrannsakan eller beslag, eftersom det kan tänkas situationer då målsäganden inte anser det vara i dennes intresse att medverka, exempelvis om även denne begått något brott. Konventionens reglering syftar emellertid inte till att förelägganden ska riktas mot målsägande. Av den förklarande rapporten framgår att föreläggandet enligt artikel 19.4 i första hand är avsett att riktas mot systemadministratörer (p. 200–202).

Det är således tillräckligt att det i den nationella lagstiftningen finns regler som ålägger en person som skulle ha kunnat höras som vittne i en rättegång att medverka. Det är mot den bakgrunden även vår uppfattning att svensk rätt formellt sett genom möjligheten att under en förundersökning hålla vittnesförhör inför rätta uppfyller de krav som ställs upp i artikel 19.4. I sammanhanget bör nämnas att Danmark vid tillträdet till konventionen inte införde några särskilda regler mot bakgrund av artikel 19.4, utan hänvisade till den möjlighet som finns i dansk rätt att under en förundersökning hålla vittnesförhör inför rätta (se Forslag til Lov om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven [IT-kriminalitet mv.], s. 48).

Det kan emellertid tänkas situationer då det kan vara svårt för den som varken är misstänkt eller målsägande och som innehar upplysningar och är villig att medverka, att avgöra om informationen fritt kan lämnas ut. Möjligheten att under en förundersökning hålla förhör med vittnen inför rätta är i sig också ett tämligen omständligt och inte särskilt snabbt sätt att få tillgång till information som skyndsamt kan behövas under en husrannsakan. Eftersom förfarandet kräver medverkan av rätten kan det inte sällan gå så lång tid innan vittnesförhöret kan hållas att bevisningen hinner förstöras. Förfarandet förutsätter dessutom att det finns någon som är skäligen misstänkt, vilket inte behöver vara fallet i det skede av utredningen då husrannsakan vidtas. Det förhållandet att den misstänkte ska ges

tillfälle att närvara vid förhöret innebär också att det finns en uppenbar risk för att förundersökningen skadas.

Enligt uppgifter som vi inhämtat anser brottsutredande myndigheter att det, för att möjliggöra husrannsakan i it-miljö, finns ett stort praktiskt behov av att kunna ge föreläggande att lämna ut viss information. Enligt polis och åklagare är det visserligen så att, när husrannsakan vidtas och behov av att genomsöka en dator eller datorsystem finns, systemadministratörer och andra personer med kunskap om datorsystemet ofta frivilligt medverkar och hjälper polisen i arbetet. Erfarenheten är vidare att när frivillig medverkan inte kommer till stånd, handlar det inte sällan om situationer där den person som innehar kunskapen om datorsystemet själv är den som kan misstänkas för brottet. Att införa en möjlighet till föreläggande att lämna information skulle inte lösa denna motsättning, eftersom ett föreläggande, mot bakgrund av bl.a. artikel 6 i Europakonventionen och förbudet mot *self-incrimination* i FN:s konvention om medborgerliga och politiska rättigheter, aldrig skulle kunna riktas mot den som är misstänkt för brottet. Erfarenheten är dock att det ändå relativt ofta uppstår situationer när den som innehar den information i form av lösenord, åtkomstkoder och dyl. som behövs för att genomföra husrannsakan och inte samtidigt är den som kan misstänkas för brottet vägrar att samarbeta.

På senare år har det växt fram ett stort antal företag, vilka hyr ut servrar eller serverutrymme för exempelvis fillagring eller i syfte att anonymisera sina kunder. De erbjuder alltså lagringsplatser för data och omfattas därför inte av regleringen i LEK. Åklagares uppfattning är att de elektroniska spåren i många brottsutredningar, exempelvis när det gäller olika former av immaterialrättsintrång, leder till sådana s.k. hostingföretag. Hos dessa kan husrannsakan användas för att söka efter föremål som får tas i beslag eller för att utröna omständigheter som kan vara av betydelse för brottsutredningen. Erfarenheten är att systemadministratörer och andra personer med kunskap om datorsystemet av lojalitet mot sina kunder eller av andra skäl inte sällan vägrar att samarbeta och att de brottsutredande myndigheterna är i behov av ett verksamt påtryckningsmedel för att få dessa att exempelvis lämna ut lösenord och åtkomstkoder eller att ange i vilken av de servrar som de innehar som de uppgifter som myndigheterna söker efter finns. I praktiken kan ett hostingföretag nämligen inneha hundratals servrar och det kan vara en omöjlig uppgift för polisen att leta igenom samtliga dessa på plats eller ta dem i beslag. Att ta samtliga servrar i beslag skulle dessutom förmodligen

i många fall strida mot proportionalitetsprincipen. Utan ett verkningsfullt påtryckningsmedel blir en husrannsakan mot ett sådant företag ofta resultatlös och de uppgifter myndigheten eftersöker riskerar att förstöras eller ändras innan de kunnat säkras.

Mot den angivna bakgrunden anser vi att det, trots att de svenska reglerna om vittnesförhör inför rätta under en förundersökning alltså formellt sett kan anses uppfylla kraven i artikel 19.4, finns skäl att överväga att i svensk rätt införa en specifik möjlighet till föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö.

I sammanhanget bör nämnas att Datastraffutredningen i betänkandet *Information och den nya informationsteknologin – straff- och processrättsliga frågor m.m.* föreslog att en sådan möjlighet till föreläggande skulle införas (SOU 1992:110, se särskilt s. 416–418 och 621–623) och att Norge, vid konventionstillträdet, mot bakgrund av artikel 19.4 införde en ny bestämmelse i *straffeprosessloven*, § 199, av innebörd att polisen vid husrannsakan i ett datasystem kan förelägga envar som är skyldig att vittna i saken att lämna de upplysningar som behövs för tillgång till datasystemet. Den som vägrar att lämna upplysningar straffas i norsk rätt med böter enligt samma bestämmelse i domstolloven, § 206, som gäller för vittnen som vägrar yttra sig.

5.4.8 Insamling i realtid av trafikuppgifter (artikel 20)

Bedömning: Svensk rätt uppfyller genom bestämmelserna om hemlig övervakning av elektronisk kommunikation konventionens krav på insamling av trafikuppgifter i realtid, om förbehåll avges av innehåll att åtgärderna i artikel 20 dels endast tillämpas på sådana brott avseende vilka hemlig övervakning av elektronisk kommunikation kan användas, dels inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt.

Skälen för bedömningen

Artikel 20 innehåller bestämmelser om insamling i *realtid* av *trafikuppgifter*. För vad som enligt konventionen är att anse som trafikuppgifter hänvisas till artikel 1 d samt avsnitt 5.2 och 5.4.4.

Enligt *punkt 1 a* ska myndigheter i en fördragsslutande stat ha rätt att med tekniska hjälpmedel insamla eller ta upp trafikuppgifter som hör till särskilt angivna meddelanden som överförs med hjälp av ett datorsystem. Enligt *punkt 1 b* ska även en tjänsteleverantör kunna åläggas att, inom ramen för vad som är tekniskt möjligt för denne, antingen själv insamla eller ta upp trafikuppgifter eller samarbeta med och biträda myndigheterna med insamling eller upptagning av trafikuppgifter.

Insamlingen eller upptagningen gäller enbart trafikuppgifter som hör till meddelanden som överförs inom statens eget territorium. Detta villkor anses vara uppfyllt om någon av dem som kommunicerar med varandra (en fysisk person eller en dator) befinner sig på statens territorium eller om kommunikationen äger rum via en dator eller telekommunikationsutrustning som befinner sig på territoriet (se den förklarande rapporten p. 222).

Av *punkt 2* framgår att en fördragsslutande stat inte behöver följa punkt 1 a, om det inte är möjligt på grund av gällande principer i statens nationella rättsordning. Staten får i så fall vidta andra åtgärder för att säkerställa insamling eller upptagning av sådana trafikuppgifter som avses.

Enligt *punkt 3* ska en tjänsteleverantör kunna åläggas att hålla hemligt att trafikuppgifter insamlas eller tas upp. Tystnadsplikt gäller också för information som har samband med förfarandet.

För de befogenheter och förfaranden som avses i artikel 20 ska enligt *punkt 4*, liksom för samtliga konventionens processrättsliga artiklar, bestämmelserna i artiklarna 14 och 15 gälla. Insamling eller upptagning av trafikuppgifter i realtid som hör till särskilt angivna meddelanden ska således som huvudregel vara möjligt vid utredningar av dels brott som straffbeläggs i enlighet med konventionen, dels andra brott som begåtts med hjälp av ett datorsystem samt även generellt vid insamling av bevis i elektronisk form om ett brott (se artikel 14.2). Av artikel 14.3 a framgår emellertid, som nämnts i avsnitt 5.4.2, att en fördragsslutande stat 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 staten tillämpar de åtgärder som avses i artikel 21 och som gäller avlyssning av innehållsuppgifter.

Insamling i realtid av trafikuppgifter är i svensk rätt möjlig genom bestämmelserna i 27 kap. rättegångsbalken om *hemlig övervakning av elektronisk kommunikation*.

Hemlig övervakning av elektronisk kommunikation innebär, som även redogjorts för i avsnitt 5.4.4, att det i hemlighet hämtas in uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits, samt får sådana meddelanden hindras från att nå fram (27 kap. 19 §).

Hemlig övervakning av elektronisk kommunikation får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader samt vid förundersökning om dataintrång enligt 4 kap. 9 c § brottsbalken, barnpornografibrott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, narkotikabrott enligt 1 § narkotikastrafflagen (1968:64) eller narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling. Hemlig övervakning av elektronisk kommunikation får också användas vid misstanke om försök, förberedelse eller stämpling till ovannämnda brott, om en sådan gärning är straffbelagd.

Hemlig övervakning av elektronisk kommunikation prövas av domstol (27 kap. 21 § första stycket). Kan det befaras att inhämtande av rättens tillstånd till hemlig övervakning av elektronisk kommunikation skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden emellertid ges av åklagaren i avvaktan på rättens beslut (27 kap. 21 a §). När tillstånd till hemlig övervakning av elektronisk kommunikation har lämnats, får användas de tekniska hjälpmedel som behövs (27 kap. 25 § första stycket).

Som huvudregel får hemlig övervakning av elektronisk kommunikation användas endast om någon är skäligen misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen om brottet. Tvångsmedlet får emellertid även användas i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Övervakning som innebär att uppgifter hämtas in om meddelanden får dock i detta fall endast avse vissa allvarligare brott och enbart avse förfluten tid (27 kap. 20 § andra stycket).

Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet (27 kap. 21 § andra stycket). Tiden kan förlängas på begäran av åklagaren. Åtgärden får avse ett telefonnummer eller annan adress eller en viss elektro-

nisk kommunikationsutrustning 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 ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

För hemlig övervakning av elektronisk kommunikation gäller, som vid all tvångsmedelsanvändning, att åtgärden i fråga får beslutas endast om skälen för åtgärden uppväger det intrång och men som åtgärden innebär för den misstänkte eller något annat motstående intresse (27 kap. 1 § tredje stycket).

Hemlig övervakning av elektronisk kommunikation kan alltså användas för att samla in sådana trafikuppgifter, dvs. uppgifter om ett meddelandes ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av tjänst, i realtid som avses i artikel 20. Det svenska tvångsmedlet kan inte användas i alla de brottsutredningar som förutsätts enligt artikel 14.2. När det gäller exempelvis brotten i konventionens straffrättsliga del har vi i tidigare avsnitt gjort bedömningen att svensk rätt uppfyller konventionens krav på kriminalisering av brotten främst genom bestämmelserna om dataintrång, brytande av post- eller telehemlighet, skadegörelse, sabotage, urkundsförfalskning, datorbedrägeri och barnpornografibrott. Av dessa kan hemlig övervakning av elektronisk kommunikation enbart användas vid förundersökning om dataintrång, grovt sabotage, grov urkundsförfalskning, grovt bedrägeri och barnpornografibrott.

De brottsbekämpande myndigheternas möjligheter att få tillgång till uppgifter om elektronisk kommunikation har under senare år setts över, bl.a. inom ramen för Beredningen för rättsväsendets utveckling (BRU) (se delbetänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* [SOU 2005:38]) och Polismetodutredningen (se delbetänkandet *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen* [SOU 2009:1]). Delar av BRU:s och Polismetodutredningens arbete behandlades i prop. 2011/12:55, i vilken en rad förändringar föreslogs i de bestämmelser som dittills gällt de brottsbekämpande myndigheternas tillgång till uppgifter som angår särskilda elektroniska meddelanden. Syftet med förändringarna var att stärka rättssäkerheten och integritetsskyddet vid inhämtning av övervakningsuppgifter (prop. 2011/12:55 s. 67). I propositionen föreslogs även att hemlig övervakning av elektronisk kommunikation i vissa fall skulle få användas

utan krav på koppling till en skäligen misstänkt person och vidare att åklagare i brådskande fall skulle få möjlighet att interimistiskt ge tillstånd till hemlig övervakning av elektronisk kommunikation (prop. 2011/12:55 s. 71–76 och s. 78–79). Regeringens förslag till lagändringar antogs av riksdagen och trädde i kraft den 1 juli 2012.

Reglerna för hemlig övervakning av elektronisk kommunikation har alltså nyligen setts över. Regering och riksdag har därvid, med beaktande av den avvägning mellan brottsbekämpningsintressen och integritetsskyddsintressen som måste göras, tagit ställning till under vilka förutsättningar tvångsmedlet ska få användas.

Som nämnts, finns möjlighet att avge förbehåll avseende artikel 20 av innehåll att åtgärderna i artikeln endast tillämpas på brott eller brottstyper som anges i förbehållet, så länge omfattningen av brotten eller brottstyperna i förbehållet inte är mer begränsad än det urval av brott på vilka staten tillämpar de åtgärder som avses i artikel 21. Artikel 21 innehåller bestämmelser om avlyssning av innehållsuppgifter. Enligt artikeln behöver åtgärderna i artikeln enbart tillämpas på vissa allvarliga brott som bestäms i de fördragsslutande staternas nationella lagstiftning. Avlyssning av innehållsuppgifter är i svensk rätt möjligt genom rättegångsbalkens bestämmelser om hemlig avlyssning av elektronisk information (se vidare avsnitt 5.4.9).

Hemlig avlyssning av elektronisk kommunikation får användas vid förundersökning som avser ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller försök, förberedelse eller stämpling till ett sådant brott, om sådan gärning är belagd med straff, samt vid förundersökning som gäller ett brott med lägre straffminimum, om brottets straffvärde bedöms överstiga fängelse i två år. Kraven för att få använda hemlig avlyssning av elektronisk kommunikation är således strängare än de som gäller för användningen av hemlig övervakning av elektronisk kommunikation. Hemlig övervakning av elektronisk kommunikation kan alltså användas i förundersökning avseende samtliga de brott där hemlig avlyssning av elektronisk kommunikation kan användas och i förundersökning avseende ytterligare ett antal brott med lägre straffminimum än vad som krävs för hemlig avlyssning av elektronisk kommunikation. Det finns således inte något hinder mot att Sverige använder sig av den möjlighet till förbehåll som artikel 14.3 a erbjuder, eftersom omfattningen av de brott på vilken hemlig övervakning av elektronisk kommunikation kan tillämpas inte är mer begränsad än det urval av brott på vilka hemlig avlyssning av elektronisk kommunikation kan tillämpas. I sammanhanget kan nämnas att såväl Danmark, Finland

som Norge avgett förbehåll av detta slag och att insamling i realtid av trafikuppgifter på det sätt som föreskrivs i artikel 20 i dessa länder alltså inte kan användas i alla de fall som avses i artikel 14.2.

Hemlig övervakning av elektronisk kommunikation får som huvudregel användas endast om någon är skäligen misstänkt för brott. Sedan den 1 juli 2012 får tvångsmedlet emellertid, som framgått, även under vissa förutsättningar användas i syfte att utreda vem som skäligen kan misstänkas för brottet. I fråga om uppgifter som rör ett särskilt meddelande får dock inhämtningen endast avse historiska uppgifter. För sådan hemlig övervakning som är av intresse för frågan om svensk rätt lever upp till konventionens krav i artikel 20 – insamling i *realtid* av trafikuppgifter – gäller således alltjämt krav på skälig misstanke. Frågan är om detta innebär något problem i förhållande till konventionsåtagandet. I artikel 20 anges visserligen inte uttryckligen att krav på skälig misstanke får uppställas. Enligt konventionen står det emellertid generellt de fördragsslutande staterna fritt att införa de åtgärder som konventionen kräver på ett sätt som passar in i respektive stats nationella rättssystem. Det är oundvikligen så att de olika rättssystemen i varierande grad kommer att innehålla olika villkor för de tvångsåtgärder som konventionen föreskriver. Konventionen förutsätter vidare att de fördragsslutande staternas nationella rättssystem innehåller olika former av rättssäkerhetsgarantier för de olika åtgärder som ska införas. Varje fördragsslutande stat har att avgöra vilka dessa bör vara i det nationella rättsystemet (se artikel 14 och 15 samt p. 215 i den förklarande rapporten). Vi anser därför inte att kravet i svensk rätt på skälig misstanke för användningen av hemlig övervakning av elektronisk kommunikation kommer i konflikt med konventionsåtagandet i artikel 20. Av samma skäl anser vi inte heller att kravet i svensk rätt på att åtgärden, dvs. den hemliga övervakningen, ska vara av synnerlig vikt för utredningen om brottet för att få användas, står i konflikt med konventionsåtagandet. Enligt vår uppfattning innebär dessa villkor för användningen av tvångsmedlet, i kombination med de för all tvångsmedelsanvändning allmänna principerna om ändamål, behov och proportionalitet samt de för hemliga tvångsmedel särskilda rättssäkerhetsmekanismerna (bl.a. Säkerhets- och integritetsskyddsnämndens arbete), i stället att svensk rätt uppfyller de krav som konventionen ålägger en fördragsslutande stat enligt artiklarna 14 och 15.

I sammanhanget kan nämnas att i *finsk rätt* är den grundläggande förutsättningen för teleövervakning (vilket är den finska motsvarigheten till det svenska tvångsmedlet hemlig övervakning av elektro-

nisk kommunikation) att någon är skäligen misstänkt för brottet. Ytterligare en förutsättning för teleövervakning är att åtgärden kan antas vara av synnerlig vikt för utredningen av brottet. Vid tillträdet till konventionen gjorde Finland bedömningen att bestämmelserna om teleövervakning uppfyllde förpliktelserna enligt artikel 20 och att några lagändringar således inte krävdes (se den finska regeringens proposition RP 153/2006 rd s. 38). Även i *norsk rätt* krävs för användning av den norska motsvarigheten till hemlig övervakning av elektronisk kommunikation – ”*kommunikasjonskontroll*” – att någon är skäligen misstänkt för brottet. Vidare krävs att tvångsmedlet är av väsentlig betydelse för utredningen och utredningen annars försvåras i väsentlig grad. Inte heller i Norge gjordes några ändringar i dessa regler vid konventionstillträdet (se Datakrimutvalgets betänkande *Lovtiltak mot datakriminalitet*, NOU 2003:27, s. 49 och den norska propositionen Ot.prp. nr. 40, [2004–2005] s. 22).

Tillstånd till hemlig övervakning av elektronisk kommunikation lämnas i svensk rätt av domstol. Artikel 20 innehåller inte något uttryckligt krav på att förfarandet ska vara skyndsamt, men det ligger i sakens natur att åtgärden ska kunna vidtas utan tidsutdräkt. Som framgått, finns i svensk rätt sedan den 1 juli 2012 en möjlighet för åklagare att i brådskande fall fatta beslut om hemlig övervakning av elektronisk kommunikation utan föregående domstolsprövning.

Hemlig övervakning av elektronisk kommunikation får i svensk rätt inte avse meddelanden som endast överförs eller har överförts i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt (27 kap. 20 § tredje stycket rättegångsbalken).

Före den 1 juli 2012 användes i stället för begreppet *meddelande* i rättegångsbalkens bestämmelser om hemlig övervakning av elektronisk kommunikation (tidigare benämnt hemlig teleövervakning) och hemlig avlyssning av elektronisk kommunikation (tidigare benämnt hemlig teleavlyssning) begreppet *telemeddelande*. Dessutom användes i stället för begreppet *elektroniskt kommunikationsnät* begreppet *telenät*. När de nya begreppen infördes i lagen var avsikten inte att dessa skulle medföra att de aktuella tvångsmedlen skulle ges en större räckvidd än tidigare i fråga om vilka meddelanden som får avlyssnas eller övervakas (prop. 2011/12:55 s. 59 och 61).

När den nämnda regeln som begränsar tillämpningsområdet för de hemliga tvångsmedlen ursprungligen infördes, angavs målet med

den vara att åstadkomma en ordning som inskränkte tvångsmedlens användning till i huvudsak sådana telekommunikationer som befordras via telenät som har någon betydelse för telesystemet som helhet (prop. 1994/95:227 s. 27). Det angavs därför att från tillämpningsområdet borde undantas områden för telekommunikationer som är särskilt integritetskänsliga eller som annars får anses tillhöra den privata sfären. Begränsningsregeln syftade till att från tillämpningsområdet för hemlig teleövervakning och hemlig teleavlyssning undanta exempelvis ”intern telekommunikation i och intill en bostad via t.ex. snabbtelefoner, porttelefoner, PC-nät och liknande utrustning” samt ”hörselslingor för hörselskadade och interna system för personsökning i form av fasta installationer” (prop. 1994/95:227 s. 27). Även interna telekommunikationer på mindre arbetsplatser avsågs falla utanför tillämpningsområdet men inte om teleadressen utnyttjades för kommunikation genom ett allmänt tillgängligt telenät eller om det gällde ett större företagsnät. Tvångsåtgärder skulle få användas om det var fråga om fristående datorer som var försedda med modem eller datorer i t.ex. små interna nätverk som via andra nätverk kommunicerade med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem. Om telekommunikationen endast skedde internt inom ett slutet nät borde det, enligt förarbetena, krävas att nätet var av större omfattning för att en tvångsåtgärd skulle få äga rum (prop. 1994/95:227 s. 31). Frågan huruvida ett telenät skulle anses vara av mindre betydelse eller inte skulle prövas utifrån en samlad bedömning av de olika omständigheter som rör ett telenäts betydelse från allmän kommunikationssynpunkt. Hur en viss utrustning fungerade och faktiskt användes var två viktiga omständigheter vid prövningen (prop. 1994/95:227 s. 31).

Som angetts i avsnitt 5.4.2, finns det enligt artikel 14.3 b möjlighet för en fördragsslutande stat att förbehålla sig rätten att inte tillämpa de tvångsmedel som avses i artikel 20 eller 21 på meddelanden som överförs inom ett datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät samt inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

I promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att det nuvarande undantaget i svensk rätt för nät av mindre betydelse från allmän kommunikationssynpunkt måste göras snävare för att Sverige ska uppfylla åtagandena i konventionen (Ds 2005:6 s. 317). Det föreslogs därför att enbart sådana nät som

saknar betydelse från allmän kommunikationssynpunkt skulle undantas.

Undantagsmöjligheten enligt konventionen måste dock ses i ljuset av att konventionen avser att täcka olika nationella begränsningar. Obligatoriet tar sikte på framför allt kommunikation i allmänna nät. Enligt vår uppfattning kommer den svenska begränsningsregeln, mot bakgrund av de redovisade förarbetsuttalandena, i allt väsentligt att omfatta sådana meddelanden som avses i artikel 14.3 b.

Som framgått, ska det enligt artikel 20.1 b vara möjligt att ålägga en tjänsteleverantör att insamla eller ta upp, eller att samarbeta med och biträda myndigheterna med insamling eller upptagning av trafikuppgifter i realtid. Med *tjänsteleverantör* avses enligt konventionens artikel 1 c en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst.

I 6 kap. 19 § LEK finns bestämmelser som knyter an till rättegångsbalkens regler om hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation och som reglerar anpassningsskyldigheten för operatörerna. Bestämmelsen innebär att vissa verksamheter ska bedrivas så att beslut om dessa tvångsmedel dels kan verkställas, dels kan verkställas under sådana former att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

Anpassningsskyldigheten enligt LEK omfattar verksamheter som avser tillhandahållande *antingen* av ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, *eller* av tjänster inom ett allmänt kommunikationsnät vilka består av *endera* 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 en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

I svensk rätt omfattar alltså anpassningsskyldigheten inte samtliga verksamheter där sådana meddelanden som omfattas av hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation befordras. Frågan om en ytterligare

anpassningsskyldighet med hänsyn till teknikutvecklingen har berörts i olika sammanhang.[13]

Det är inte alldeles tydligt om kretsen av de aktörer som ska kunna åläggas att samarbeta med de brottsutredande myndigheterna enligt konventionen helt motsvarar den krets som omfattas av anpassningsskyldigheten enligt LEK. Vår mening är att den möjliga skillnaden mellan konventionens reglering och den svenska regleringen när det gäller anpassningsskyldigheten för operatörerna i varje fall inte är så omfattande att det är nödvändigt att föreslå några lagändringar i denna del för att kunna tillträda konventionen.

Enligt 6 kap. 21 § LEK har leverantörerna tystnadsplikt för uppgift om bl.a. hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation. Tystnadsplikten gäller även om det nät eller den tjänst som leverantören tillhandahåller inte är allmänt respektive allmän (jfr regleringen i 6 kap. 19 § LEK om anpassningsskyldigheten). Tillämpningsområdet är vidare inte begränsat till leverantören utan också andra aktörer omfattas av tystnadsplikten, t.ex. den som på uppdrag av leverantören utför delar av tillhandahållandet av nätet eller tjänsten (se om detta Post- och telestyrelsens [PTS] ”*Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter*”, 2006-11-28). Reglerna om tystnadsplikt i LEK har, som framgått i avsnitt 5.4.4, företräde framför den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen Enligt vår mening är bestämmelserna tillräckliga för att uppfylla konventionskravet i artikel 20.3.

Sammanfattningsvis är det alltså vår uppfattning att om Sverige avger förbehåll av innehåll att åtgärderna i artikel 20 dels endast tillämpas på sådana brott avseende vilka hemlig övervakning av elektronisk kommunikation kan användas, dels inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt, krävs inte några lagstiftningsåtgärder för att uppfylla konventionskraven i artikel 20.

[13] Se bl.a. Beredningens för rättsväsendets utveckling (BRU) förslag i delbetänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38, s. 281–284) och vissa anmärkningar som Utredningen om vissa hemliga tvångsmedel avslutningsvis gjorde i sitt delbetänkande *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44, s. 770).

5.4.9 Avlyssning av innehållsuppgifter (artikel 21)

Bedömning: Svensk rätt uppfyller genom bestämmelserna om hemlig avlyssning av elektronisk kommunikation konventionens krav på avlyssning av innehållsuppgifter, om förbehåll avges av innehåll att åtgärderna i artikel 21 inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt.

Skälen för bedömningen

Artikel 21 innehåller bestämmelser om *avlyssning* av *innehållsuppgifter*.

Enligt *punkt 1 a* ska myndigheter i en fördragsslutande stat, med avseende på vissa allvarliga brott som bestäms i statens nationella lagstiftning, ha rätt att med tekniska hjälpmedel i realtid insamla eller ta upp innehållsuppgifter i särskilt angivna meddelanden som överförs med hjälp av ett datorsystem. Enligt *punkt 1 b* ska även en tjänsteleverantör kunna åläggas att i realtid, inom dennes existerande tekniska förmåga, antingen själv insamla eller ta upp innehållsuppgifter eller samarbeta med och biträda myndigheterna med insamling eller upptagning av sådana uppgifter. Insamlingen eller upptagningen gäller, på samma sätt som beträffande insamling av trafikuppgifter i realtid, enbart uppgifter i meddelanden som överförs inom statens eget territorium (se avsnitt 5.4.8 när detta villkor anses uppfyllt).

Av *punkt 2* framgår att en fördragsslutande stat inte behöver följa punkt 1 a, om det inte är möjligt på grund av gällande principer i statens nationella rättsordning. Staten får i så fall vidta andra åtgärder för att säkerställa insamling eller upptagning av sådana innehållsuppgifter som avses.

Enligt *punkt 3* ska en tjänsteleverantör kunna åläggas att hemlighålla det förhållandet att innehållsuppgifter insamlas eller tas upp och vidare all information som har samband med förfarandet.

Avlyssning av innehållsuppgifter är i svensk rätt möjlig genom bestämmelserna i 27 kap. rättegångsbalken om *hemlig avlyssning av elektronisk kommunikation*.

Hemlig avlyssning av elektronisk kommunikation innebär, som även redogjorts för i avsnitt 5.4.4, att meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett visst telefonnummer eller en annan adress avlyssnas eller tas upp

i hemlighet genom ett tekniskt hjälpmedel (27 kap. 18 §). Hemlig avlyssning av elektronisk kommunikation får användas vid förundersökning som avser ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller försök, förberedelse eller stämpling till ett sådant brott, om sådan gärning är belagd med straff, samt vid förundersökning som gäller ett brott med lägre straffminimum, om brottets straffvärde bedöms överstiga fängelse i två år. Ett tillstånd till hemlig avlyssning av elektronisk kommunikation ger också rätt att hämta in sådana övervakningsuppgifter som annars är åtkomliga med stöd av ett tillstånd till hemlig övervakning av elektronisk kommunikation.

Hemlig avlyssning av elektronisk kommunikation prövas, liksom hemlig övervakning av elektronisk kommunikation av domstol (27 kap. 21 § första stycket). När tillstånd till hemlig avlyssning av elektronisk kommunikation har lämnats, får de tekniska hjälpmedel som behövs användas (27 kap. 25 § första stycket). Någon motsvarande möjlighet för åklagare som när det gäller hemlig övervakning av elektronisk kommunikation att i brådskande fall enligt rättegångsbalken utan föregående domstolsprövning besluta om åtgärden finns inte när det gäller hemlig avlyssning av elektronisk kommunikation.[14] Även för hemlig avlyssning av elektronisk kommunikation gäller att tvångsmedlet får användas endast om någon är skäligen misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen om brottet.

Tiden för tillstånd till hemlig avlyssning av elektronisk kommunikation får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet (27 kap. 21 § andra stycket). Tiden kan förlängas på begäran av åklagaren. Åtgärden får, på samma sätt som när det gäller hemlig övervakning av elektronisk kommunikation, avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning 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 ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att

[14] En möjlighet för åklagare att interimistiskt ge tillstånd till hemlig avlyssning av elektronisk kommunikation finns dock enligt 2008 års utredningslag. Som nämnts i avsnitt 5.4.4 har Utredningen om vissa hemliga tvångsmedel i betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) vidare föreslagit att åklagare ska ges möjlighet att i brådskande fall fatta beslut även om hemlig avlyssning av elektronisk kommunikation.

anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta (27 kap. 20 §).

För hemlig avlyssning av elektronisk kommunikation gäller, som vid all tvångsmedelsanvändning, att åtgärden i fråga får beslutas endast om skälen för åtgärden uppväger det intrång och men som åtgärden innebär för den misstänkte eller något annat motstående intresse (27 kap. 1 § tredje stycket).

De bestämmelser i LEK som redogjorts för i avsnitt 5.4.8 och som gäller leverantörers anpassningsskyldighet och tystnadsplikt gäller även vid beslut om hemlig avlyssning av elektronisk kommunikation.

Hemlig avlyssning av elektronisk kommunikation kan alltså användas för att i realtid ta upp innehållsuppgifter på det sätt som avses i artikel 21. Att tvångsmedlet i svensk rätt enbart kan användas i förundersökning om brott med högt straffminimum eller straffvärde är förenligt med konventionsåtagandet, eftersom det står varje fördragsslutande stat fritt att avgöra vid vilka brott avlyssning av innehållsuppgifter ska kunna användas.

I svensk rätt kan hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation endast användas om dels någon skäligen är misstänkt för brott, dels åtgärden är av synnerlig vikt för utredningen om brottet. Som framgått i det föregående avsnittet utgör detta inte något problem i förhållande till det konventionsåtagande som följer av artikel 20. Motsvarande bedömning görs avseende artikel 21.

Att domstol enligt rättegångsbalken måste ge tillstånd till hemlig avlyssning av elektronisk kommunikation är förenligt med åtagandet enligt artikel 21. Något uttryckligt krav på att förfarandet ska vara skyndsamt finns inte i artikeln och på flera ställen i den förklarande rapporten (se bl.a. p. 210, 212 och 215) erkänns den uppfattning som finns i många stater, däribland Sverige, om att avlyssning av innehållsuppgifter är extra känsligt ur integritetssynpunkt och därför bör vara omgärdat av speciella regler som garanterar rättssäkerheten.

På samma sätt som när det gäller hemlig övervakning av elektronisk kommunikation, får i svensk rätt hemlig avlyssning av elektronisk kommunikation inte avse meddelanden som endast överförs eller har överförts i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt (27 kap. 20 § tredje stycket rättegångsbalken).

Vi har i avsnitt 5.4.8 gjort den bedömningen att om möjligheten till förbehåll enligt artikel 14.3 utnyttjas, krävs ingen ändring av begränsningsregeln i 27 kap. 20 § tredje stycket rättegångsbalken för att motsvara konventionskraven såvitt gäller artikel 20 om insamling i realtid av trafikuppgifter. Vi har vidare gjort bedömningen att de svenska reglerna om operatörers anpassningsskyldighet är förenliga med konventionens reglering enligt artikel 20. Vi gör motsvarande bedömningar såvitt avser artikel 21.

Enligt vår mening är bestämmelserna i LEK och offentlighets- och sekretesslagen (2009:400) om tystnadsplikt för leverantörer tillräckliga för att uppfylla konventionskravet i artikel 21.3.

Sammanfattningsvis är det alltså vår uppfattning att om Sverige avger förbehåll av innehåll att åtgärderna i artikel 21 inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt, krävs inte några lagstiftningsåtgärder för att uppfylla konventionskraven i artikel 21.

5.5 Domsrätt (artikel 22)

Bedömning: De allmänna svenska domsrättsreglerna i 2 kap. brottsbalken uppfyller kraven enligt konventionen. Det finns inte någon anledning att för svensk del göra förbehåll om inskränkning av domsrätten.

Skälen för bedömningen

I *artikel 22* finns bestämmelser om domsrätt.

Enligt artikel *22.1* ska de fördragsslutande staterna säkerställa att de har domsrätt över brotten enligt artiklarna 2–11 när brottet begåtts (a) på den fördragsslutande statens territorium, (b) på ett fartyg som förde statens flagg (c) ombord på ett luftfartyg registrerat i den ifrågavarande staten, och (d) när brottet begåtts av en medborgare i den fördragsslutande staten, om brottet är straffbart enligt strafflagstiftningen där det begicks eller om brottet inte faller under någon stats territoriella behörighet.

Av artikel *22.2* följer att en fördragsslutande stat 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–c i artikeln eller en del av dessa regler.

De svenska bestämmelserna om domsrätt finns huvudsakligen i 2 kap. brottsbalken. Reglerna om domsrätt är vidsträckta och det finns generellt goda möjligheter att ingripa även mot brott som har begåtts utomlands.

Svensk domsrätt föreligger alltid när brottet är begånget i Sverige (1 §) eller på ett svenskt fartyg eller luftfartyg (3 § 1). Ett brott anses begånget där den brottsliga handlingen utfördes men också där brottet fullbordades eller, vid försök, där brottet skulle ha fullbordats (4 §). Av detta följer att svensk lag fullt ut motsvarar de krav som följer av artikel 22.1 a–c.

För domsrätt över brott begångna av svenska medborgare utomlands uppställs krav på s.k. dubbel straffbarhet. Från kravet finns vissa undantag bl.a. när det gäller barnpornografibrott som består i att skildra barn i pornografisk bild och grovt barnpornografibrott. Kravet på dubbel straffbarhet innebär att domsrätten förutsätter att gärningen inte var fri från ansvar enligt lagen på gärningsorten eller, om den begåtts inom ett område som inte tillhör någon stat, att svårare straff än böter kan följa på gärningen (2 § första stycket 1 och andra stycket). För samtliga de brott som i svensk rätt motsvarar brotten i artiklarna 2–11 kan följa svårare straff än böter. Svensk lag motsvarar därför fullt ut även de krav som följer av artikel 22.1 d. Sverige har således inte något behov av att göra ett sådant förbehåll som avses i punkt 2 i artikeln.

Enligt artikel *22.3* ska en fördragsslutande stat ha domsrätt när en påstådd gärningsman befinner sig på statens territorium och staten endast på grund av den misstänktes nationalitet inte utlämnar honom eller henne till en annan fördragsslutande stat. Regleringen ger i denna del uttryck för principen *aut dedere aut judicare* – antingen utlämna eller lagföra. Den situation det främst är fråga om är således den om Sverige skulle vägra utlämna någon på grund av att han eller hon är svensk medborgare. Svensk domsrätt föreligger då i första hand enligt den tidigare nämnda bestämmelsen i 2 kap. 2 § första stycket 1 brottsbalken, alternativt enligt bestämmelsen i 2 kap. 2 § första stycket 2 brottsbalken, vilken utvidgar den svenska jurisdiktionen till utlänningar som efter att ha begått brott utomlands blivit svenska medborgare eller tagit hemvist här. Det är nämligen förhållandena vid tidpunkten för gärningen som är avgörande för frågan om medborgarskapet enligt jurisdiktionsreglerna (se Berggren m.fl., *Brottsbalken En kommentar Kap. 1–12*, s. 2:20). För frågan

om medborgarskap förhindrar utlämning är emellertid den kritiska tidpunkten den då utlämning ska ske (prop. 1913:50 s. 28 och 1957:156 s. 40). Tidpunkten för brottets förövande är alltså i detta avseende ovidkommande för utlämningsfrågan.

Den situationen skulle också kunna tänkas då Sverige vägrar utlämna någon på grund av att han eller hon är medborgare i en annan nordisk stat.[15] Domsrätt föreligger då, om brottet inte begåtts i Sverige, enligt antingen 2 kap. 2 § första stycket 1 (utlänning med hemvist i Sverige) eller 2 brottsbalken (utlänning utan hemvist i Sverige som är dansk, finsk, isländsk eller norsk medborgare och finns här).

Svensk lag uppfyller alltså även de krav som följer av artikel 22.3.

I artikel *22.4* anges att konventionen inte utesluter straffrättslig domsrätt som utövas i enlighet med nationell lagstiftning.

Artikel *22.5* stadgar om samråd i fall av positiva kompetenskonflikter.

Varken artikel 22.4 eller 22.5 kräver någon lagstiftning.

Sammanfattningsvis är det alltså vår bedömning att de allmänna svenska domsrättsreglerna i 2 kap. brottsbalken uppfyller de krav som följer av konventionen.

5.6 Bestämmelser om internationellt samarbete

5.6.1 Allmänt om bestämmelserna

Bestämmelserna om internationellt samarbete utgör en stor del av konventionen. De är uppdelade i två avsnitt, ett allmänt avsnitt där de grundläggande principerna läggs fast och ett med särskilda bestämmelser om vissa tvångsåtgärder m.m.

Det allmänna avsnittet är uppdelat i olika avdelningar som behandlar allmänna principer för hela det rättsliga samarbetet enligt konventionen (artikel 23), principer som gäller för utlämning (artikel 24) respektive rättslig hjälp (artiklarna 25 och 26) samt bestäm-

[15] Det föreligger inte något hinder enligt lagen (1957:668) om utlämning för brott (utlämningslagen) att utlämna annan nordisk medborgare, men Sverige har avgett en förklaring till den europeiska utlämningskonventionen av den 13 december 1957 av innebörd att för svensk del förstås med medborgare i den konventionens mening – förutom svenska medborgare – bl.a. medborgare i Danmark, Finland, Island och Norge. Regeringen kan alltså med stöd av den diskretionära rätt att antingen bevilja eller vägra utlämning som följer av utlämningslagen, även i förhållande till en annan stat som anslutit sig till utlämningskonventionen, vägra utlämning på grund av att den som eftersöks för utlämning är medborgare i en annan nordisk stat.

melser beträffande förfarandet vid framställningar om rättslig hjälp (artiklarna 27 och 28).

Det andra avsnittet är indelat i avdelningar som behandlar rättslig hjälp med provisoriska åtgärder (artiklarna 29 och 30), rättslig hjälp med utredningsbefogenheter (artiklarna 31–34) och nätverk av kontaktpunkter (artikel 35).

5.6.2 Allmänna principer för internationellt samarbete (artikel 23)

Bedömning: Bestämmelserna i artikel 23 får anses ge uttryck för mera allmänna principer för samarbetet. Artikeln medför mot den bakgrunden inte något behov av lagstiftningsåtgärder för att Sverige ska kunna tillträda konventionen.

Skälen för bedömningen

I *artikel 23* anges vilka allmänna principer som ska gälla för det internationella samarbetet om utredning eller lagföring av brott som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller insamling av bevis i elektronisk form om brott.

Enligt artikeln ska de fördragsslutande staterna i största möjliga utsträckning samarbeta med varandra i enlighet med konventionens bestämmelser om internationellt samarbete samt genom tillämpning av

- relevanta internationella instrument om internationellt samarbete i straffrättsliga frågor,
- gällande överenskommelser som ingåtts på grundval av ensartad eller reciprok lagstiftning, och
- nationella lagar.

Bestämmelserna i artikel 23 ger uttryck för mera allmänna principer för samarbetet. Avsikten är att vad som mer allmänt gäller internationellt straffrättsligt samarbete ska gälla även it-relaterad brottslighet. Artikeln medför inte något behov av lagstiftningsåtgärder för att Sverige ska kunna tillträda konventionen.

5.6.3 Principer för utlämning (artikel 24)

Bedömning: Konventionens bestämmelser om utlämning medför inget krav på lagstiftning.

Skälen för bedömningen

I *artikel 24* regleras frågor om utlämning.

Enligt *punkt 1 a* ska artikeln tillämpas på utlämning mellan fördragsslutande stater för brott som straffbeläggs i enlighet med artiklarna 2-11 i konventionen, om brotten enligt lagstiftningen i båda staterna kan straffas med frihetsberövande och maximistraffet uppgår till lägst ett år.

Om det emellertid följer av en överenskommelse eller ett utlämningsavtal som gäller mellan två eller flera av de fördragsslutande staterna att ett annat lägsta straff ska tillämpas ska, enligt *punkt 1 b*, det lägsta straff som anges i en sådan överenskommelse eller ett sådant avtal i stället gälla mellan de inblandade staterna.

Av *punkt 2* följer att de fördragsslutande staterna åtar sig att säkerställa att brotten som avses i punkt 1 är att anse som utlämningsbara enligt både nu befintliga och framtida utlämningsavtal mellan dem.

Punkt 3 gäller stater som, till skillnad från Sverige, för utlämning ställer som villkor att det finns ett utlämningsavtal och innebär att konventionen ska kunna utgöra rättslig grund för utlämning i dessa fall. I varje fall ska, enligt *punkt 4*, staterna erkänna brott som anges i punkt 1 som utlämningsbara.

Enligt *punkt 5* ska för utlämning gälla de villkor som anges i den anmodade statens lagstiftning eller i gällande utlämningsavtal, inklusive de skäl på grund av vilka den anmodade staten får vägra utlämning.

Eftersom Sverige inte uppställer krav på avtal för att utlämning ska kunna beviljas är det i detta sammanhang den svenska lagstiftningen som är av intresse.

Förutsättningarna för utlämning respektive överlämnande regleras i lagen (1957:668) om utlämning för brott (utlämningslagen) respektive lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder (europeiska arresteringsorderlagen) och lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder (nordiska arresteringsorderlagen).

Vad beträffar strafftrösklarna gäller för utlämning enligt utlämningslagen att det för brottet är stadgat fängelse i ett år eller mer enligt *svensk* lag (4 §).[16] Är fråga om överlämnande enligt den europeiska arresteringsorderlagen gäller som huvudregel ett krav på att gärningen motsvarar brott enligt svensk lag och att det för brottet är föreskrivet fängelse ett år eller mer i den *utfärdande* statens lagstiftning (2 kap. 2 § första stycket 1). Enligt den nordiska arresteringsorderlagen gäller inte något krav på dubbel straffbarhet. Överlämnande får ske när den eftersökte är misstänkt, tilltalad eller dömd för en brottslig gärning för vilken det är föreskrivet en frihetsberövande påföljd i den *utfärdande* staten (2 kap. 2 § första stycket).

Som framgår i avsnitt 5.3 gör vi bedömningen att de kriminaliseringskrav som följer av konventionen i huvudsak uppfylls av nu befintliga straffbestämmelser. Endast när det gäller datorrelaterad förfalskning (artikel 7) anser vi att det krävs lagstiftningsåtgärder för att möjliggöra ett svenskt tillträde till konventionen. Som vi har redovisat i avsnitt 5.3.8 har regeringen i proposition 2012/13:74 *Förfalsknings- och sanningsbrotten* lämnat förslag till ett nytt urkundsbegrepp i 14 kap. 1 § brottsbalken som, om det antas av riksdagen, innebär att svensk rätt genom bestämmelsen om urkundsförfalskning kommer att uppfylla konventionskravet även i denna del.

Såväl tillämpliga befintliga straffbestämmelser som den av regeringen föreslagna ändrade kriminaliseringen av urkundsförfalskning uppfyller samtidigt de krav som ställs för att brotten ska vara utlämningsbara. Något behov av ytterligare lagstiftning för att uppfylla kraven på utlämningsbarhet i artikel 24 kan därför inte anses finnas.

Enligt *punkt 6* ska en stat som enbart på grund av den eftersökta personens nationalitet eller därför att staten anser sig ha domsrätt över brottet vägrar utlämning för ett brott som avses i punkten 1, efter framställning från den ansökande staten hänskjuta ärendet till sina behöriga myndigheter för lagföring. Dessa myndigheter ska fatta beslut och genomföra utredning och lagföring på samma sätt som för andra brott av jämförbar natur enligt nationell lagstiftning. Slutresultatet ska sedan rapporteras till den ansökande staten.

Om Sverige, genom en ansökan om utlämning, får information om att en person som har begått ett brott eller misstänks ha begått ett brott enligt konventionen befinner sig inom landet, men hinder mot utlämning föreligger exempelvis på grund av att personen är svensk medborgare, finns regelmässigt ett intresse från svensk sida

[16] Utlämningsutredningen har i sitt förslag till ny utlämningslag inte föreslagit någon ändring av detta villkor (se SOU 2011:71 s. 461–467).

att utreda förutsättningar för åtal för gärningen i fråga. Vidare finns i 23 kap. rättegångsbalken regler om när förundersökning ska inledas. Bestämmelserna innebär bl.a. att polismyndighet eller åklagare, om det finns anledning att anta att ett brott som hör under allmänt åtal har begåtts, ska fatta beslut om att inleda en förundersökning.

På motsvarande sätt gäller, enligt 20 kap. 6 § rättegångsbalken, att åklagare är skyldig att åtala brott som hör under allmänt åtal om inte något annat är särskilt föreskrivet.

Det nu anförda innebär att det inte kan anses krävas några författningsändringar för att Sverige ska uppfylla de krav som följer av punkt 6 (jfr regeringens bedömning av behovet av författningsändringar vid tillträdet till Europarådets konvention om förebyggande av terrorism, prop. 2009/10:78 s. 35–36).

Punkt 7 innebär enbart att varje fördragsslutande stat ska meddela Europarådets generalsekreterare vilka nationella myndigheter som är ansvariga för att göra och ta emot framställningar om utlämning eller provisoriskt frihetsberövande i avsaknad av avtal, och att generalsekreteraren ska upprätta och föra en aktuell förteckning över dessa myndigheter.

Sammanfattningsvis medför alltså konventionens bestämmelser om utlämning inget krav på lagstiftning.

5.6.4 Allmänna principer för ömsesidig rättslig hjälp (artikel 25)

Bedömning: Konventionens bestämmelser om allmänna principer för rättslig hjälp medför inget krav på lagstiftning.

Skälen för bedömningen

I *artikel 25* anges vilka allmänna principer som ska gälla för rättslig hjälp.

Enligt *punkt 1* ska de fördragsslutande staterna 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.

Av *punkt 2* följer att varje fördragsslutande stat ska vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att uppfylla åtagandena i artiklarna 27-35.

Enligt *punkt 3* får en fördragsslutande stat i brådskande fall göra framställningar om ömsesidig rättslig hjälp eller sända meddelande relaterade därtill genom snabba kommunikationsmedel, så som telefax eller elektronisk post, i den mån sådana medel tillgodoser tillräckliga säkerhetsnivåer och verifiering med efterföljande formell bekräftelse, i den mån den anmodade staten kräver det. Den anmodade staten ska i det sammanhanget godta och besvara framställningar genom sådana snabba kommunikationsmedel.

Om inte något annat uttryckligen föreskrivs i konventionen ska, enligt *punkt 4*, för ömsesidig rättslig hjälp gälla de villkor som föreskrivs i den anmodade statens lagstiftning eller i tillämpliga avtal om ömsesidig rättslig hjälp, inklusive de skäl på grund av vilka den anmodade staten får avslå en framställning om samarbete. Den anmodade staten får emellertid inte vägra rättslig hjälp i fråga om brott som avses i artiklarna 2-11 i konventionen enbart av det skälet att framställningen gäller ett brott som den anser vara ett fiskalt brott.

Enligt *punkt 5* ska, i de fall där den anmodade staten i enlighet med bestämmelserna i konventionen, har rätt att uppställa krav på dubbel straffbarhet som villkor för rättslig hjälp, det villkoret anses uppfyllt, oberoende av hur den anmodade staten kategoriserar brottet, så länge gärningen utgör brott i nationell lagstiftning.

Bestämmelserna i artikel 25 ger, liksom bestämmelserna i artikel 23, huvudsakligen uttryck för sådana mera allmänna principer för samarbetet som redan är etablerade.

Bestämmelser om rättslig hjälp finns i lagen (2000:562) om internationell rättslig hjälp i brottmål (Lirb). I sammanhanget bör framhållas att den svenska lagstiftningen är generös och syftar till att ge utländska brottsbekämpande myndigheter tillgång till samma verktyg som svenska åklagare och domstolar, i princip oberoende av om en framställning om hjälp baseras på avtal eller inte.

Någon vägransgrund hänförlig till att fråga är om ett fiskalt brott innehåller Lirb inte. En ansökan om rättslig hjälp i Sverige ska enligt Lirb göras skriftligen genom post, bud eller telefax men får även, efter överenskommelse i det enskilda fallet, översändas på annat sätt (2 kap. 4 § fjärde stycket).

För de fall Sverige uppställer krav på dubbel straffbarhet för rättslig hjälp är det tillräckligt att den gärning som ansökan avser *motsvarar* ett brott enligt svensk lag (2 kap. 2 § Lirb). Det krävs

alltså inte att den gärning som ansökan avser ska falla direkt under en svensk straffbestämmelse utan det är tillräckligt att den aktuella gärningstypen är kriminaliserad i Sverige (se prop. 1999/2000:61 s. 189, jfr prop. 1978/79:80 s. 15–17 och NJA 1993 s. 137).

Sammanfattningsvis medför artikeln alltså inte något behov av lagstiftningsåtgärder för att Sverige ska kunna tillträda konventionen.

5.6.5 Upplysningar som lämnas på eget initiativ (artikel 26)

Bedömning: Bestämmelserna om informationsutbyte på eget initiativ medför inget behov av lagstiftning.

Skälen för bedömningen

I *artikel 26* finns bestämmelser om informationsutbyte på eget initiativ, dvs. informationsutbyte som inte sker med anledning av en ansökan om rättslig hjälp eller annan framställning.

Enligt *punkt 1* får en fördragsslutande stat, inom gränserna för sin nationella lagstiftning och utan föregående framställning, överlämna information som erhållits inom ramen för dess egna utredningar till en annan fördragsslutande stat, när den anser att sådan information skulle kunna hjälpa den mottagande staten att inleda eller genomföra utredningar och rättsliga förfaranden om brott som är straffbara enligt konventionen, eller som skulle kunna föranleda en framställning om samarbete från den staten enligt bestämmelserna om internationellt samarbete i konventionen.

Av *punkt 2* framgår att den stat som lämnar information får ställa upp villkor om hemlighållande och användningsbegränsning samt att den mottagande staten ska vara bunden av sådana villkor i den utsträckning den nationella lagstiftningen medger det.

Ytterst är det, som framgått, nationell rätt som bestämmer utrymmet för sådant informationsutbyte som avses i artikeln.

Svenska myndigheter kan i dag frivilligt lämna information till en annan stat – med de begränsningar som gäller med hänsyn till sekretess – och då ställa villkor som begränsar den mottagande statens användning av uppgifterna (se bl.a. prop. 2009/10:78 s. 37).

I de fall då en svensk myndighet är tilltänkt mottagare av informationen finns bestämmelser om bindande villkor om användningsbegränsningar i 5 kap. 1 § Lirb. För polisiärt samarbete finns

särskilda bestämmelser om bindande användningsbegränsningar i 3 § lagen (2000:343) om internationellt polisiärt samarbete och 4 kap. 2 § lagen (2000:1219) om internationellt tullsamarbete.

När det gäller uppgifter i ett ärende om internationell rättslig hjälp i brottmål gäller 18 kap. 17 § offentlighets- och sekretesslagen (2009:400). Sekretess gäller för uppgift i verksamhet som avser rättsligt samarbete på begäran av bl.a. en annan stat, för uppgift som hänför sig till en utredning enligt bestämmelserna om förundersökning i brottmål eller en angelägenhet som angår tvångsmedel, om det kan antas att det varit en förutsättning för den andra statens begäran att uppgiften inte skulle röjas. Skaderekvisitet har formulerats så att den utländska myndigheten i viss mån får förfoga över frågan om sekretess, så länge det är fråga om sekretess som inte sträcker sig längre än vad som kunnat förekomma i en motsvarande svensk utredning (prop. 1999/2000:61 s. 168). Mot bakgrund av att det inom det straffrättsliga samarbetet är en självklar utgångspunkt att känsliga uppgifter i den utländska brottsutredningen kan skyddas i den anmodade staten råder enligt uttalanden i förarbetena en stark presumtion för sekretess (prop. 1999/2000:61 s. 209).

Någon lagstiftning fordras inte på grund av innehållet i artikel 26.

5.6.6 Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal (artikel 27)

Bedömning: Bestämmelserna om förfaranden vid framställningar om rättslig hjälp i avsaknad av tillämpliga internationella avtal medför inget behov av lagstiftning. Något skäl för Sverige att kräva att samtliga framställningar om rättslig hjälp ska ställas till Centralmyndigheten finns inte.

Skälen för bedömningen

I *artikel 27* finns procedurregler för framställningar om rättslig hjälp.

Bestämmelserna i artikeln är, enligt *punkt 1*, tillämpliga enbart om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp mellan de berörda fördragsslutande staterna, eller om staterna, trots att det finns ett sådant avtal eller en sådan överens-

kommelse, kommer överens om att tillämpa någon eller några av artikelns bestämmelser.

Enligt *punkt 2* ska de fördragsslutande staterna utse en eller flera centralmyndigheter som ska svara för att sända och besvara framställningar om ömsesidig rättslig hjälp, handlägga sådana framställningar eller överlämna dem till de behöriga myndigheterna för handläggning. Centralmyndigheterna ska kommunicera direkt med varandra. Varje fördragsslutande stat ska meddela Europarådets generalsekreterare vilken som är dess centralmyndighet och generalsekreteraren ska föra en aktuell förteckning över centralmyndigheterna.

Av *punkt 3* framgår att framställningar om ömsesidig rättslig hjälp enligt artikeln ska göras i enlighet med det förfarande som anges av den ansökande staten, om detta inte är oförenligt med den anmodade statens lagstiftning.

Som anges i artikel 25.4 är konventionens huvudregel att för ömsesidig rättslig hjälp ska gälla de villkor och grunder för avslag som föreskrivs i den anmodade statens lagstiftning (se avsnitt 5.6.4). Enligt *punkt 4* har en anmodad stat dessutom rätt att avslå en framställning om rättslig hjälp om framställningen gäller ett brott som den betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller om den anser att verkställande av framställningen kan antas inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper (*ordre public*) eller andra viktiga intressen.

I *punkt 5* klargörs att den anmodade staten kan skjuta upp verkställandet av en begärd åtgärd, om denna skulle skada dess myndigheters brottsutredningar eller rättsliga förfaranden. Det betyder att den anmodade statens egna anspråk har företräde.

Innan samarbete med annan fördragsslutande stat vägras eller skjuts upp måste emellertid enligt *punkt 6* den anmodade staten, där så är lämpligt efter att ha samrått med den ansökande staten, överväga om framställningen kan bifallas partiellt eller på vissa villkor som den bedömer som nödvändiga.

Den anmodade staten ska, enligt *punkt 7*, genast underrätta den ansökande staten om utfallet av en framställning om rättslig hjälp. Om en begäran om samarbete helt eller delvis avslagits eller uppskjutits ska den anmodade staten ange skälen för sitt beslut. Den anmodade staten ska också underrätta den ansökande staten om skäl som gör det omöjligt att verkställa framställningen eller kan antas komma att försena verkställandet avsevärt.

Enligt *punkt 8* kan den ansökande staten kräva att den anmodade staten sekretessbelägger en framställning om rättslig hjälp och dess innehåll utom i den omfattning som behövs för att verkställa framställningen. Om den anmodade staten inte kan uppfylla detta sekretesskrav ska den genast underrätta den ansökande staten om detta, varvid denna har att avgöra om framställningen ändå ska verkställas.

I brådskande fall får enligt *punkt 9* framställningar om ömsesidig rättslig hjälp eller därtill hörande meddelanden skickas direkt mellan staternas rättsliga myndigheter (dvs. åklagare eller domare, se den förklarande rapporten p. 274). Om så sker ska dock den ansökande statens centralmyndighet samtidigt sända en kopia av framställningen eller meddelandet till den anmodade statens centralmyndighet. Vidare får sådana framställningar och meddelanden översändas genom Interpol. Är den myndighet som har tagit emot framställningen inte behörig, ska framställningen lämnas över till den myndighet som är behörig samtidigt som den ansökande staten underrättas. Avser framställningen samarbete som inte innefattar användning av tvångsmedel ska framställningar och meddelanden alltid kunna sändas direkt mellan de berörda myndigheterna i respektive stat, oavsett om ärendet är brådskande eller inte. En fördragsslutande stat får emellertid meddela Europarådets generalsekreterare att framställningar om rättslig hjälp, oavsett om de är brådskande eller inte, av effektivitetsskäl alltid ska ställas direkt till dess centralmyndighet.

Även enligt andra internationella konventioner som har utarbetats för det straffrättsliga samarbetet ska tillträdande stater utse en centralmyndighet för att ta emot och sända framställningar. Centralmyndighetsfunktionen är för svenskt vidkommande sedan den 1 oktober 2000 placerad i Justitiedepartementet som en del av departementets enhet för brottmålsärenden och internationellt rättsligt samarbete (BIRS).[17]

En ansökan om internationell rättslig hjälp i Sverige ska enligt 2 kap. 6 § Lirb ges in till Justitiedepartementet som lämnar ansökan till Åklagarmyndigheten eller till behörig domstol (enligt 2 kap. 7 § första stycket Lirb som huvudregel den tingsrätt inom vars område den begärda åtgärden ska vidtas), om inte ansökan ska prövas av

[17] Centralmyndighetsfunktionen i Justitiedepartementet har nyligen varit föremål för en övergripande översyn (Ju 2011:A). I uppdraget har bl.a. legat att överväga den framtida placeringen av Centralmyndigheten. Efter att den översynen slutfördes har en utredare fått i uppdrag att fortsätta arbetet och föreslå var centralmyndighetsfunktionen ska vara placerad (Ju 2012:M). Utredaren ska redovisa sitt uppdrag i form av en promemoria under hösten 2013.

regeringen. En ansökan från en stat som är medlem i EU eller från Island, Norge eller Schweiz får dock göras direkt hos behörig åklagare eller domstol. Så får ske även i andra fall när det finns en internationell överenskommelse om det.

Enligt 2 kap. 7 § tredje stycket Lirb ska om det kommer fram att en åklagare eller tingsrätt inte är behörig att handlägga ansökan denna överlämnas till behörig åklagare eller tingsrätt.

De svenska reglerna innebär inte något hinder mot att kommunikation sker direkt mellan de berörda myndigheterna i fråga om samarbete som inte innefattar tvångsåtgärder (jfr 1 kap. 2 § andra stycket Lirb).

Om en ansökan inte innehåller de uppgifter som behövs för handläggningen ska, enligt 2 kap. 9 § Lirb, den ansökande staten ges tillfälle att komplettera ansökan. Vidare ska, om en ansökan kan bifallas endast delvis eller under vissa villkor, den ansökande staten underrättas om de hinder som finns och ges tillfälle att yttra sig eller komplettera eller ändra ansökan.

Ansökningar om rättslig hjälp ska, enligt 2 kap. 10 § Lirb, behandlas skyndsamt. Som huvudregel ska tillämpas samma förfarande som när en motsvarande åtgärd vidtas vid en svensk förundersökning eller rättegång. Innehåller en ansökan en begäran om ett visst förfarande ska vidare, enligt 2 kap. 11 § Lirb, detta tillämpas, om inte det begärda förfarandet strider mot grundläggande principer i den svenska rättsordningen.

Enligt 2 kap. 16 § Lirb ska ett beslut om att avslå en ansökan innehålla de skäl som bestämt utgången.

När handläggningen av ärendet har avslutats ska det, enligt 2 kap. 17 § Lirb, redovisas till Justitiedepartementet för vidarebefordran till den ansökande staten. Har ansökan gjorts direkt hos behörig åklagare eller domstol ska ärendet emellertid redovisas direkt till den ansökande myndigheten.

De svenska regler som nu nämnts är alltså i överenstämmelse med konventionens bestämmelser i artikel 27.2, 27.3, 27.6, 27.7 och 27.9. Något skäl för Sverige att kräva att samtliga framställningar om rättslig hjälp ska ställas till Centralmyndigheten finns inte.

I 2 kap. 14 § första stycket Lirb anges att en ansökan om rättslig hjälp *ska* avslås, om ett bifall till ansökan skulle kränka Sveriges suveränitet, medföra fara för rikets säkerhet eller strida mot svenska allmänna rättsprinciper eller andra väsentliga intressen. Denna grund för avslag är den enda obligatoriska avslagsgrunden enligt Lirb. Mot bakgrund av artikel 27.4 möter det inte något hinder att

avslå en begäran om samarbete med stöd av denna obligatoriska avslagsgrund.

En ansökan om rättslig hjälp *får* enligt 2 kap. 14 § andra stycket Lirb också avslås om (1) gärningen har karaktär av ett politiskt brott, (2) om gärningen utgör ett militärt brott (om inte gärningen motsvarar även annat brott enligt svensk lag vilket inte är ett militärt brott) eller (3) om det i Sverige har meddelats dom eller beslut om åtalsunderlåtelse beträffande gärningen. Slutligen finns en möjlighet att (4) avslå en ansökan, om omständigheterna annars är sådana att ansökan inte bör bifallas.

Avslagsgrunderna i 2 kap. 14 § andra stycket Lirb är alltså fakultativa och får, enligt bestämmelsens tredje stycke, inte tillämpas i den mån de skulle strida mot en internationell överenskommelse som gäller mellan Sverige och den ansökande staten. Om Sverige tillträder Europarådets konvention om it-relaterad brottslighet och ett avslag skulle strida mot konventionen får det således inte beslutas. Som framgått, är konventionens huvudregel emellertid att för ömsesidig rättslig hjälp ska gälla de villkor och grunder för avslag som föreskrivs i den anmodade statens lagstiftning och den svenska avslagsgrunden om politiskt brott har dessutom uttryckligt stöd i artikel 27.4.

Regleringen i artikel 25.4 och 27.4 innebär alltså att såväl den obligatoriska avslagsgrunden som de fakultativa avslagsgrunderna i Lirb är förenliga med konventionen.

Som redogjorts för i avsnitt 5.6.5 gäller enligt 18 kap. 17 § offentlighets- och sekretesslagen (2009:400) sekretess för uppgift i verksamhet som avser rättsligt samarbete på begäran av bl.a. en annan stat, för uppgift som hänför sig till en utredning enligt bestämmelserna om förundersökning i brottmål eller en angelägenhet som angår tvångsmedel, om det kan antas att det varit en förutsättning för den andra statens begäran att uppgiften inte skulle röjas. Skaderekvisitet har alltså formulerats så att den utländska myndigheten i viss mån får förfoga över frågan om sekretess. Regleringen uppfyller de krav som ställs i artikel 27.8.

Bestämmelsen i artikel 27.5 om att den anmodade statens egna anspråk har företräde framför en ansökan om rättslig hjälp, innebär inte någon förpliktelse och kräver således inte någon lagstiftningsåtgärd.

Sammanfattningsvis medför artikel 27 alltså inte några krav på lagändringar.

5.6.7 Sekretess och begränsningar i fråga om användning (artikel 28)

Bedömning: Bestämmelserna om sekretess och begränsningar i fråga om användning medför inget behov av lagstiftning.

Skälen för bedömningen

Artikel 28 innebär en möjlighet för den anmodade staten att uppställa dels krav på sekretess dels s.k. specialitetsförbehåll.

Bestämmelserna i artikeln är, enligt *punkt 1*, enbart tillämpliga om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp mellan de berörda fördragsslutande staterna, eller om staterna, trots att det finns ett sådant avtal eller en sådan överenskommelse, kommer överens om att tillämpa någon eller några av artikelns bestämmelser.

Enligt *punkt 2* får den anmodade staten 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 (specialitetsförbehåll).

Enligt *punkt 3* ska den ansökande staten, om den inte kan uppfylla ett sådant villkor som anges i punkt 2, genast meddela den anmodade staten, som då har att avgöra om upplysningarna ändå kan lämnas. Om den ansökande staten däremot godtar ett villkor är den bunden av det.

En fördragsslutande stat som lämnar upplysningar eller material med ett sådant förbehåll som anges i punkt 2 får, enligt *punkt 4*, begära att den andra staten förklarar hur den har använt upplysningarna eller materialet med avseende på detta villkor.

I avsnitt 5.6.5 har redogjorts för bestämmelsen i 18 kap. 17 § offentlighets- och sekretesslagen (2009:400) om sekretess för uppgift i verksamhet som avser rättsligt samarbete på begäran av bl.a. en annan stat. Regleringen innebär att Sverige, som ansökande stat, kan uppfylla de krav på hemlighållande som avses i artikel 28.2 a.

Som nämnts i avsnitt 5.6.5 finns bestämmelser om bindande villkor om användningsbegränsningar i 5 kap. 1 § Lirb. Om uppgifter eller bevisning har överlämnats från en annan stat till en svensk myndighet för att användas vid utredning av brott eller i ett rätts-

ligt förfarande med anledning av brott, gäller enligt den bestämmelsen att myndigheten ska följa de begränsningar som den andra staten ställer upp oavsett vad som annars är föreskrivet i lag eller annan författning. För polisiärt samarbete finns särskilda bestämmelser om bindande användningsbegränsningar i 3 § lagen (2000:343) om internationellt polisiärt samarbete och 4 kap. 2 § lagen (2000:1219) om internationellt tullsamarbete. Med stöd av bestämmelserna kan svenska myndigheter således tillmötesgå en begäran om användningsbegränsningar från en annan fördragsslutande stat.

Sammanfattningsvis medför artikel 28 alltså inget behov av lagstiftning.

5.6.8 Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter (artikel 29)

Bedömning: Det krävs lagstiftning för att uppfylla konventionens krav på rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter.

Skälen för bedömningen

Artikel 29 behandlar rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter. Bestämmelsen reglerar således rättslig hjälp med sådant säkrande som avses i artikel 16.

Enligt *punkt 1* får en fördragsslutande stat anmoda en annan fördragsslutande stat att genom föreläggande eller på annat sätt åstadkomma skyndsamt säkrande av uppgifter som lagrats med hjälp av ett datorsystem inom den anmodade statens territorium och beträffande vilka den ansökande staten avser att överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av uppgifterna.

Av *punkt 2* framgår att en framställning om säkrande enligt punkt 1 ska innehålla:

- namnet på den myndighet som begär säkrandet,
- den gärning som är föremål för brottsutredning eller lagföring och ett sammandrag av omständigheterna,

- de lagrade datorbehandlingsbara uppgifter som ska säkras och deras förhållande till brottet,
- alla tillgängliga upplysningar som identifierar den som förvarar de lagrade datorbehandlingsbara uppgifterna eller var datorsystemet finns,
- upplysning om varför säkrandet är nödvändigt, samt
- uppgift om att den ansökande staten avser att överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av de lagrade datorbehandlingsbara uppgifterna.

Enligt *punkt 3* ska den anmodade staten, när den mottar en framställning om säkrande, vidta alla lämpliga åtgärder för att skyndsamt säkra de särskilt angivna uppgifterna i enlighet med sin nationella lagstiftning. Villkor om dubbel straffbarhet ska inte uppställas för säkrandet.

En fördragsslutande stat 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 dock enligt *punkt 4*, med avseende på andra brott än de som avses i artiklarna 2–11, förbehålla sig rätten att avslå en framställning om säkrande om den har skäl att tro att villkoret om dubbel straffbarhet inte kan uppfyllas när uppgifterna ska röjas.

Skälet till artikelns reglering om att krav på dubbel straffbarhet inte ska uppställas, är dels att ett säkrande ska kunna ske snabbt, utan att den anmodade staten ska lägga tid på att utreda om den aktuella gärningen motsvarar ett brott enligt den nationella lagstiftningen, dels att den säkrandeåtgärd som det är fråga om inte anses vara en särskilt ingripande åtgärd, eftersom uppgifterna som säkras inte samtidigt ska röjas (se den förklarande rapporten p. 285).

I övrigt får en framställning om säkrande enligt *punkt 5* avslås endast om framställningen gäller ett brott som den anmodade staten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller om denna anser att verkställandet av framställningen kan antas inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper (*ordre public*) eller andra viktiga intressen.

Enligt *punkt 6* ska den anmodade staten, om denna anser att ett säkrande inte kommer att trygga den framtida tillgängligheten till

uppgifterna eller kommer att hota sekretessen för eller på annat sätt störa den ansökande statens brottsutredning, genast meddela den ansökande staten som har att avgöra om framställningen ändå ska verkställas.

Ett säkrande som verkställs som svar på en sådan framställning som avses i punkt 1 ska enligt *punkt 7* gälla under en period om minst 60 dagar, för att den ansökande staten ska kunna överlämna en framställning om husrannsakan eller liknande åtkomst, beslag eller liknande säkringsåtgärd eller röjande av uppgifterna. När en sådan framställning mottagits ska vidare uppgifterna bevaras i avvaktan på ett beslut om framställningen.

Vi har i avsnitt 5.4.4 gjort bedömningen att det krävs lagstiftning för att uppfylla konventionens krav på skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 16. Eftersom det i en svensk förundersökning alltså inte är möjligt att få till stånd ett sådant skyndsamt säkrande som avses i artikel 16 är det heller inte möjligt att ge annan stat rättslig hjälp med sådant säkrande. Det krävs därför, som framhållits, lagstiftning även för att uppfylla konventionens krav på rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29.

I sammanhanget bör uppmärksammas att dubbel straffbarhet inte får uppställas som krav för rättslig hjälp med det säkrande som avses i artikeln, i vart fall inte för sådana brott som är upptagna i artiklarna 2–11. I svensk rätt krävs som huvudregel dubbel straffbarhet för lämnande av rättslig hjälp med tvångsmedel eller tvångsåtgärder. Rättslig hjälp med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation får således lämnas endast om krav på dubbel straffbarhet är uppfyllt (2 kap. 2 § Lirb). Även för rättslig hjälp med husrannsakan och beslag krävs som huvudregel dubbel straffbarhet. Endast om den ansökande staten är annan medlemsstat i EU, Island, Norge eller Schweiz krävs inte att gärningen motsvarar ett brott enligt svensk lag (2 kap. 2 § jfr med 4 kap. 20 § Lirb). För att uppfylla kraven i artikel 29 krävs således att det i en framtida reglering om rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter inte ställs upp krav på dubbel straffbarhet.

5.6.9 Skyndsamt röjande av säkrade trafikuppgifter (artikel 30)

Bedömning: Det krävs lagstiftning för att uppfylla konventionens krav på rättslig hjälp med skyndsamt röjande av säkrade trafikuppgifter.

Skälen för bedömningen

Artikel 30 behandlar skyndsamt röjande av trafikuppgifter då flera tjänsteleverantörer har varit inblandade i överföringen av sådana uppgifter som ska säkras enligt artikel 29. Liksom enligt artikel 17 syftar röjandet av trafikuppgifterna enbart till att identifiera vilka övriga tjänsteleverantörer som deltagit vid överföringen, så att uppgifter kan säkras även hos dessa.

Enligt *punkt 1* ska den anmodade staten om den, 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 överföringen av meddelandet snabbt för den ansökande staten röja den mängd trafikuppgifter som behövs för att identifiera tjänsteleverantören och den väg på vilken meddelandet överfördes.

Den tillkommande tjänsteleverantören kan antingen finnas i den ansökande staten eller i en tredje stat. Den ansökande staten har då möjlighet att antingen själv se till att uppgifter hos denna tjänsteleverantör säkras eller inge en ansökan om rättslig hjälp med säkrande av uppgifterna till den tredje staten (se den förklarande rapporten p. 290).

Den anmodade staten får enligt *punkt 2* underlåta att röja trafikuppgifter enligt punkt 1 endast om framställningen gäller ett brott som staten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller om den anser att verkställande av framställningen kan antas inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper (*ordre public*) eller andra viktiga intressen.

Vi har i avsnitt 5.4.5 gjort bedömningen att det krävs lagstiftning för att uppfylla konventionens krav på skyndsamt partiellt röjande av trafikuppgifter enligt artikel 17. Det krävs därmed också lagstiftningsåtgärder för att möjliggöra rättslig hjälp med sådant röjande.

Även i detta sammanhang bör påpekas att konventionen inte tillåter att krav på dubbel straffbarhet uppställs för sådan rättslig hjälp. De enda avslagsgrunder som är tillåtna är de som anges i punkten 2, låt vara att det i praktiken inte kan bli fråga om röjande av sådana trafikuppgifter som avses om inte de villkor som den anmodade staten uppställt för säkrande av uppgifter enligt artikel 29 är uppfyllda.

5.6.10 Ömsesidig rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter (artikel 31)

Bedömning: Bestämmelserna om rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter medför inget behov av lagstiftning.

Skälen för bedömningen

Artikel 31 behandlar rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter. Enligt den förklarande rapporten (p. 292) motsvarar artikeln rättslig hjälp med sådana åtgärder som avses i artikel 19 om husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter och som enligt den artikeln ska kunna vidtas i en nationell brottsutredning.

Enligt *punkt 1* får en fördragsslutande stat ansöka hos en annan fördragsslutande stat om hjälp med att genom husrannsakan eller på liknande sätt skaffa åtkomst till, genom beslag eller liknande åtgärd säkra eller röja uppgifter som lagrats med hjälp av ett datorsystem inom den anmodade statens territorium, däribland uppgifter som har säkrats enligt artikel 29.

Av *punkt 2* framgår att den anmodade staten ska besvara framställningen med tillämpning av de internationella instrument, överenskommelser och lagar som avses i artikel 23 (dvs. relevanta internationella instrument om internationellt samarbete i straffrättsliga frågor, andra relevanta överenskommelser och nationella lagar) och i enlighet med andra tillämpliga bestämmelser om internationellt samarbete i konventionen.

Enligt *punkt 3* ska en framställning om rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter besvaras skyndsamt när

- det finns skäl att tro att uppgifterna i fråga löper särskild risk att gå förlorade eller förändras, eller
- de instrument, överenskommelser och lagar som avses i punkt 2 på annat sätt föreskriver skyndsamt samarbete.

Vi har i avsnitt 5.4.7 gjort bedömningen att de svenska bestämmelserna om husrannsakan och beslag uppfyller de krav på sådana åtgärder som ställs i artikel 19.

Husrannsakan och beslag omfattas av de åtgärder som på ansökan av annan stat kan vidtas med stöd av Lirb. I huvudsak tillämpas samma förfarande som när en motsvarande åtgärd vidtas vid en svensk förundersökning.

Som nämnts i avsnitt 5.6.8 krävs för rättslig hjälp med husrannsakan och beslag som huvudregel dubbel straffbarhet. Endast om den ansökande staten är annan medlemsstat i EU, Island, Norge eller Schweiz krävs inte att gärningen motsvarar ett brott enligt svensk lag (2 kap. 2 § jfr med 4 kap. 20 § Lirb). Det förhållandet att Sverige alltså som huvudregel ställer upp krav på dubbel straffbarhet för vidtagande av nu aktuella åtgärder utgör inte något problem i förhållande till konventionsåtagandet (jfr artikel 23 och 25.4). Som redogjorts för i avsnitt 5.6.8 ska krav på dubbel straffbarhet, delvis av effektivitetsskäl, inte uppställas för sådan säkrandeåtgärd som avses i artikel 29. Grunderna för att vägra en ansökan om säkrande enligt artikel 29 är även i övrigt, som framgår av det nämnda avsnittet, ytterst begränsade. Det förhållandet och regleringen i artikel 31, som inte hindrar att krav på dubbel straffbarhet eller att andra villkor för rättslig hjälp med husrannsakan och beslag ställs upp i den nationella lagstiftningen, kan således innebära att uppgifter som säkrats enligt artikel 29 senare inte kan lämnas ut med stöd av artikel 31. Konventionen förutsätter att så kan bli fallet.

Husrannsakan och beslag kan, som nämnts i tidigare avsnitt (se bl.a. avsnitt 5.4.4), i svensk rätt inte användas för att få ut uppgifter om meddelanden i ett elektroniskt kommunikationsnät hos en operatör. Åtkomsten till sådana uppgifter regleras i stället exklusivt genom bestämmelserna i rättegångsbalken om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation samt till viss del, när det gäller abonnentuppgifter, genom bestämmelser i LEK. Rättslig hjälp med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation på ansökan av annan stat kan även den ske med

stöd av Lirb. Det förhållandet att svensk rätt således tillämpar en annan ordning för utfående av uppgifter från en operatör än husrannsakan och beslag innebär enligt vår mening inte något problem i förhållande till åtagandet i artikel 31, eftersom Sverige alltså *kan* bistå andra stater med åtkomst till, säkrande eller röjande av lagrade datorbehandlingsbara uppgifter även hos dessa aktörer. Som framgått ska enligt artikel 25.4, om inte annat uttryckligen föreskrivits i de särskilda artiklarna, för ömsesidig rättslig hjälp gälla de villkor som föreskrivs i den anmodade statens lagstiftning eller i tillämpliga avtal om ömsesidig rättslig hjälp (jfr härvid även artikel 23). De villkor på vilka Sverige beviljar rättslig hjälp med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation, och som innebär att det liksom enligt den nationella rätten bl.a. krävs att brottet är av visst allvar, är mot den bakgrunden förenliga med åtagandet enligt artikel 31. Som framgått utgör inte heller det förhållandet att Sverige uppställer krav på dubbel straffbarhet för rättslig hjälp med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation något problem i förhållande till artikel 31.

Enligt 2 kap. 4 § andra stycket Lirb ska en ansökande stat i samband med ansökan om rättslig hjälp ange och motivera om ärendet är brådskande eller om verkställighet önskas inom viss tidsfrist, och allmänt gäller enligt lagen att ansökningar om rättslig hjälp ska behandlas skyndsamt (2 kap. 10 §). Den svenska regleringen lever således redan upp till det skyndsamhetskrav som föreskrivs i artikel 31.3.

Sammanfattningsvis är det således vår uppfattning att bestämmelserna om rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter inte medför något behov av lagstiftning.

5.6.11 Gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter med samtycke eller i de fall de är allmänt tillgängliga (artikel 32)

Bedömning: Bestämmelserna om gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter medför inget behov av lagstiftning.

Skälen för bedömningen

Enligt *artikel 32* får en fördragsslutande stat utan tillstånd av en annan sådan stat

- bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga, oavsett var uppgifterna befinner sig geografiskt, eller
- genom ett datorsystem inom sitt territorium bereda sig åtkomst till eller ta emot lagrade datorbehandlingsbara uppgifter som finns hos annan fördragsslutande stat, om den förstnämnda staten erhåller lagligt och frivilligt samtycke av den person som har laglig rätt att röja uppgifterna för staten via det datorsystemet.

Samtycke till tvångsmedel tillerkänns generellt inte någon verkan i svensk rätt. En enskild anses inte kunna samtycka till sådant intrång i den egna sfären som kräver lagstöd enligt regeringsformen eller Europakonventionen (Lindberg, *Straffprocessuella tvångsmedel*, tredje upplagan, 2012, s. 53–54). Samtycke av den enskilde till exempelvis husrannsakan får därför inte tillmätas betydelse. I 28 kap. 1 § tredje stycket rättegångsbalken finns en uttrycklig bestämmelse om samtycke till husrannsakan. Enligt bestämmelsen får för husrannsakan hos den misstänkte inte i något fall åberopas hans eller hennes samtycke, om inte den misstänkte själv har begärt att åtgärden ska vidtas.

Artikel 32 är emellertid inte att läsa så att husrannsakan ska kunna vidtas med en misstänkts samtycke. Vilka regler som ska gälla för samtycke till tvångsåtgärder är en fråga som faller utanför konventionen och helt regleras i den nationella rätten. Artikeln medför i sig inte några egentliga förpliktelser utan är att betrakta som en överenskommelse om att tillåta en annan fördragsslutande stat att utan underrättelse eller tillstånd ta del av datorbehandlingsbara uppgifter som tekniskt sett finns på det egna territoriet. De två situationer då en stat ska kunna få åtkomst till uppgifter på en annan stats territorium, utan underrättelse eller tillstånd, som räknas upp i artikeln är situationer som alla de stater som var med och utarbetade konventionen var eniga om redan idag är folkrättsligt tillåtna (se den förklarande rapporten p. 293).

Åtkomsten till den information som avses i artikeln förutsätts inte ske genom samtycke till en tvångsåtgärd utan kan ske genom frivillig medverkan av annat slag. En målsägande som befinner sig i en stat kan exempelvis vilja ge polisen tillgång till sin elektroniska

post som finns lagrad hos en tjänsteleverantör i en annan stat. Polisen i den först nämnda staten ska då kunna bereda sig tillgång till den elektroniska posten utan att först underrätta den andra staten eller be denna om tillstånd.

Bestämmelserna om gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter är enligt vår mening okontroversiella och medför inget behov av lagstiftning.

5.6.12 Ömsesidig rättslig hjälp med insamling i realtid av trafikuppgifter (artikel 33)

Bedömning: Bestämmelserna om rättslig hjälp med insamling i realtid av trafikuppgifter medför inget behov av lagstiftning.

Skälen för bedömningen

Artikel 33 innehåller bestämmelser om rättslig hjälp med insamling i realtid av trafikuppgifter.

Enligt artikeln ska de fördragsslutande staterna 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. För denna hjälp ska gälla de villkor och förfaranden som anges i den nationella lagstiftningen. Staterna ska dock lämna sådan hjälp åtminstone med avseende på brott för vilka insamling i realtid av trafikuppgifter skulle vara möjlig i ett motsvarande nationellt fall.

Vi har i avsnitt 5.4.8 gjort bedömningen att svensk rätt genom bestämmelserna om hemlig övervakning av elektronisk kommunikation uppfyller konventionens krav på insamling i realtid av trafikuppgifter enligt artikel 20, om förbehåll av visst innehåll avges. Rättslig hjälp med såväl hemlig övervakning som hemlig avlyssning av elektronisk kommunikation omfattas av Lirb. Som nämnts i tidigare avsnitt är den svenska lagstiftningen om internationell rättslig hjälp generös och syftar till att ge utländska brottsbekämpande myndigheter tillgång till samma verktyg som svenska åklagare och domstolar.

Rättslig hjälp avseende bl.a. hemlig övervakning och hemlig avlyssning av elektronisk kommunikation ska, enligt 2 kap. 1 § första stycket Lirb, således 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 Lirb. Särskilda bestämmelser om rättslig hjälp i Sverige med hemlig övervakning och hemlig avlyssning av elektronisk kommunikation finns i 4 kap. 25 § Lirb. De särskilda bestämmelserna innebär bl.a. att svenska myndigheter inte behöver granska vilken betydelse de upptagningar eller uppteckningar som gjorts har för den utländska brottsutredningen. Den granskningen får ske av de ansökande myndigheterna efter det att ärendet har återredovisats enligt 2 kap. 17 § Lirb.

För rättslig hjälp med hemlig övervakning av elektronisk kommunikation ställs, enligt 2 kap. 2 § Lirb, krav på dubbel straffbarhet. Kravet kommer inte i konflikt med konventionens reglering (jfr artikel 25.4 och 25.5).

Eftersom kraven för beviljande av rättslig hjälp med hemlig övervakning av elektronisk kommunikation inte är strängare än de som gäller för åtgärden enligt en svensk förundersökning uppfyller svensk rätt konventionskraven i artikel 33.

5.6.13 Ömsesidig rättslig hjälp med avlyssning av innehållsuppgifter (artikel 34)

Bedömning: Bestämmelserna om rättslig hjälp med avlyssning av innehållsuppgifter medför inget behov av lagstiftning.

Skälen för bedömningen

Artikel 34 innehåller bestämmelser om rättslig hjälp med avlyssning av innehållsuppgifter.

Enligt artikeln ska de fördragsslutande staterna, 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.

Ytterst är det alltså nationell rätt och andra internationella instrument än konventionen som en stat tillträtt som bestämmer utrymmet för rättslig hjälp med avlyssning av innehållsuppgifter.

Vi har i avsnitt 5.4.9 gjort bedömningen att svensk rätt genom bestämmelserna om hemlig avlyssning av elektronisk kommunika-

tion uppfyller konventionens krav på avlyssning av innehållsuppgifter enligt artikel 21, om förbehåll av visst innehåll avges. Som nämnts i avsnitt 5.6.12 ska rättslig hjälp avseende bl.a. hemlig avlyssning av elektronisk kommunikation enligt 2 kap. 1 § första stycket Lirb, 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 Lirb. De särskilda bestämmelserna om rättslig hjälp i Sverige med hemlig övervakning och hemlig avlyssning av elektronisk kommunikation i 4 kap. 25 § Lirb, innebär, som nämnts i avsnitt 5.6.12, bl.a. att svenska myndigheter inte behöver granska vilken betydelse de upptagningar eller uppteckningar som gjorts har för den utländska brottsutredningen. När det gäller hemlig avlyssning av elektronisk kommunikation ska en sådan granskning som krävs för att iaktta förbudet mot hemlig avlyssning mellan den misstänkte och hans försvarare enligt 27 kap. 22 § rättegångsbalken dock göras. Av 5 kap. 2 § Lirb följer att åklagaren när avlyssnat material överlämnas, i den mån det inte strider mot en internationell överenskommelse, kan förena överlämnandet av materialet med villkor. Ett sådant villkor kan vara att materialet ska förstöras efter det att det rättsliga förfarandet är avslutat i den ansökande staten.

För rättslig hjälp med hemlig avlyssning av elektronisk kommunikation ställs, liksom avseende hemlig övervakning av elektronisk kommunikation, enligt 2 kap. 2 § Lirb krav på dubbel straffbarhet. Kravet kommer inte i konflikt med konventionens reglering (jfr artikel 25.4 och 25.5).

De svenska bestämmelserna om rättslig hjälp med hemlig avlyssning av elektronisk kommunikation innebär alltså att Sverige i hög utsträckning kan bistå med sådan hjälp. Svensk rätt lever därför mer än väl upp till konventionens intentioner i detta avseende. Artikel 34 medför inget behov av lagstiftning.

5.6.14 Nätverk (24/7) (Artikel 35)

Bedömning: Bestämmelsen om utseende av en kontaktpunkt medför inget behov av lagstiftning. Sverige bör utse Rikspolisstyrelsen till kontaktpunkt.

Skälen för bedömningen

Enligt *artikel 35* ska varje fördragsslutande stat utse en kontaktpunkt, med tillgång till utbildad personal och utrustning, som ska vara tillgänglig dygnet runt alla veckans dagar för att vid behov ge 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 ett brott.

Hjälpen ska innefatta underlättande av eller, om det är tillåtet i statens nationella lagstiftning och praxis, direkt vidtagande av följande åtgärder:

- tillhandahållande av teknisk rådgivning,
- säkrande av uppgifter i enlighet med artiklarna 29 och 30, samt
- insamling av bevis, tillhandahållande av rättslig information och lokalisering av misstänkta.

De fördragsslutande staternas kontaktpunkter ska skyndsamt kunna kommunicera med varandra. Vidare ska, om en utsedd kontaktpunkt inte samtidigt är den statens myndighet som ansvarar för internationell rättslig hjälp eller utlämning, kontaktpunkten skyndsamt kunna samverka med den myndighet som är ansvarig för frågan.

Hos Rikspolisstyrelsen finns sedan drygt tio år tillbaka en operativ kontaktpunkt för bekämpning av högteknologisk brottslighet. En enhet inom Rikskriminalpolisen ansvarar för it-relaterad brottslighet och har beredskap dygnet runt alla dagar i veckan, vilket innebär att det alltid går att nå en specialist på området för it-relaterade brott. Utanför kontorstid går kontakten via Rikskommunikationscentralen. Kravet i artikel 35 på en kontaktpunkt som alltid är tillgänglig kan således uppfyllas genom utseende av Rikspolisstyrelsen som kontaktpunkt. Artikel 35 medför således inget behov av lagstiftning. Det kan dock finnas skäl att, mot bakgrund av konventionsåtagandet, se över organisationen inom Rikspolisstyrelsen så att den enhet som i praktiken ska fungera som kontaktpunkt förfogar över de resurser som krävs för att fullgöra denna uppgift.

5.7 Slutbestämmelser (artiklarna 36–48)

Bedömning: Slutbestämmelserna föranleder inte några lagändringar. Det finns inte någon anledning för Sverige att specificera för vilket eller vilka territorier som konventionen ska gälla.

Skälen för bedömningen

Artiklarna 36–48 innehåller avslutande bestämmelser om bl.a. undertecknande och ikraftträdande, anslutning osv. Bestämmelserna har, med vissa undantag, utformats i enlighet med den modell för slutbestämmelser som finns för konventioner och överenskommelser inom Europarådet (se den förklarande rapporten p. 303).

Artikel 36 behandlar frågor om undertecknande och ikraftträdande. Som tidigare nämnts trädde konvention i kraft den 1 juli 2004. I relation till en enskild signatärstat träder konventionen i kraft första dagen i den månad som följer efter utgången av en period på tre månader efter den dag då signatären uttryckt sitt samtycke till att vara bunden av konventionen.

Enligt *artikel 37* kan Europarådets ministerkommitté med de fördragsslutande staternas enhälliga samtycke inbjuda andra stater, härunder också stater som inte är medlemmar av Europarådet, att ansluta sig till konventionen.

I *artikel 38* ges en fördragsslutande stat möjlighet att ange för vilket eller vilka territorier konventionen ska gälla. För svensk del finns inte någon anledning att avge någon sådan specificering.

Artikel 39 behandlar konventionens verkan bl.a. i relation till andra internationella instrument. Det anges t.ex. i artikel 39.3 att konventionen inte inverkar på en fördragsslutande stats övriga rättigheter, begränsningar, skyldigheter eller ansvar.

Artikel 40 innehåller en uppräkning av i vilken utsträckning en fördragsslutande stat kan avge förklaring att ytterligare rekvisit uppställs. Vi har behandlat möjligheterna att uppställa ytterligare rekvisit i anslutning till de bestämmelser i sak där det varit befogat att överväga en sådan förklaring. Vi återkommer i avsnitt 8 till i vilken utsträckning Sverige föreslås utnyttja möjligheten till förklaring.

Artikel 41 rör federala stater.

Artikel 42 innehåller en uttömmande uppräkning av i vilken utsträckning en fördragsslutande kan göra förbehåll mot vissa bestämmelser i konventionen. Vi har behandlat möjligheterna att göra

förbehåll i anslutning till de bestämmelser i sak där det varit befogat att överväga ett förbehåll. Vi återkommer i avsnitt 8 till i vilken utsträckning Sverige föreslås utnyttja möjligheten till förbehåll.

Artikel 43 behandlar återtagande av förbehåll.

Enligt *artikel 44* kan varje fördragsslutande stat föreslå ändringar av konventionen. Ändringsförslag ska senare enligt en viss procedur underställas de fördragsslutande staterna för antagande.

Av *artikel 45* följer att de fördragsslutande staterna ska söka lösa tvister om tolkningen eller tillämpningen av konventionen genom förhandling eller med andra fredliga medel, varvid det särskilt hänvisas till hänskjutande till Europarådets styrkommitté för brottsfrågor (CDPC), till skiljedomstol 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.

Enligt *artikel 47* kan en fördragsslutande stat när som helst säga upp konventionen genom ett meddelande ställt till Europarådets generalsekreterare.

Artikel 48, slutligen, anger de meddelanden (om undertecknande, deponering av olika instrument, ikraftträdande osv.) som ska lämnas från Europarådets generalsekreterare till bl.a. de fördragsslutande staterna.

Artiklarna 36–48 innehåller inte något som kräver lagstiftningsåtgärder.

6 Behovet av lagändringar mot bakgrund av tilläggsprotokollet

6.1 Inledning

I detta kapitel analyseras, med utgångspunkt i tilläggsprotokollets artiklar, de behov av lagändringar som tilläggsprotokollet föranleder.

6.2 Straffrättsliga bestämmelser

6.2.1 Allmänt om bestämmelserna

Tilläggsprotokollet behandlar frågan om kriminalisering av gärningar av rasistisk eller främlingsfientlig natur som begås med hjälp av datorsystem. Protokollet aktualiserar därmed frågor om informations-, yttrande- och tryckfrihet. I ingressen till tilläggsprotokollet erkänns yttrandefriheten som en av de viktigaste grundvalarna i ett demokratiskt samhälle och en grundläggande förutsättning för samhällets framåtskridande och varje människas utveckling. Behovet av att säkerställa en lämplig avvägning mellan yttrandefriheten och bekämpning av gärningar av rasistisk eller främlingsfientlig natur betonas vidare, och det framhålls att protokollet inte avser att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem. I en av tilläggsprotokollets artiklar (artikel 3.3) finns dessutom en uttrycklig hänvisning till sådana principer i nationell rätt.

Tilläggsprotokollet behandlar liksom konventionen enbart *uppsåtliga* gärningar. Vidare används begreppet *orättmätigt* (”without right”) på samma sätt som i konventionen för att avgränsa det område som ska straffbeläggas. Termer och uttryck som används i tilläggsprotokollet ska, enligt artikel 2.2, tolkas på samma sätt som i konventionen och konventionens artikel 1, som innehåller defini-

tioner, ska, enligt artikel 8.1, i tillämpliga delar gälla även för tilläggsprotokollet. Detta innebär att exempelvis ”datorsystem” är att förstå på samma sätt som enligt konventionens artikel 1 a (se avsnitt 5.2).

Här bör nämnas att i promemorian *Brott och brottsutredning i itmiljö* (Ds 2005:6) gjordes bedömningen att det inte krävdes några lagstiftningsåtgärder för att uppfylla tilläggsprotokollets straffrättsliga bestämmelser, om Sverige gjorde vissa förbehåll mot artiklarna 3, 5 och 6.

I sammanhanget bör vidare nämnas att tilläggsprotokollet i många delar överensstämmer med EU:s rambeslut 2008/913/RIF av den 28 november 2008 om bekämpande av vissa former av och uttryck för rasism och främlingsfientlighet enligt strafflagstiftningen, och att regeringen har gjort bedömningen att svensk rätt uppfyller rambeslutets krav (se regeringsbeslut den 10 april 2008 i ärende Ju2008/3200/L5).

6.2.2 Spridande av rasistiskt och främlingsfientligt material med hjälp av datorsystem (artikel 3)

Bedömning: Svensk rätt uppfyller genom främst bestämmelserna om hets mot folkgrupp och uppvigling tilläggsprotokollets krav på vad som ska vara straffbelagt som spridande av rasistiskt och främlingsfientligt material med hjälp av datorsystem.

Skälen för bedömningen

Enligt *artikel 3.1* ska det vara straffbelagt att uppsåtligt och orättmätigt sprida eller på annat sätt tillgängliggöra rasistiskt och främlingsfientligt material till allmänheten med hjälp av ett datorsystem.

Rasistiskt och främlingsfientligt material definieras i artikel 2.1 som ”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”.

Begreppet ”tillgängliggöra” anses innefatta även sådana åtgärder som att skapa eller sammanställa länkar i syfte att göra det lättare

att få tillgång till rasistiskt och främlingsfientligt material (se den förklarande rapporten p. 28).

Enligt *artikel 3.2* får en fördragsslutande stat förbehålla sig möjligheten att inte införa straffansvar när materialet i artikel 3.1 förespråkar, främjar eller uppmuntrar diskriminering *utan samband med hat eller våld*. En förutsättning för detta är att det, i stället för straffansvar, finns andra effektiva åtgärder att tillgå.

Om en stat beroende på etablerade principer om yttrandefrihet i sitt rättssystem, inte kan föreskriva vare sig straffansvar eller andra effektiva åtgärder för vissa fall av sådan diskriminering som avses i artikel 3.1, får staten, enligt *artikel 3.3*, förbehålla sig rätten att inte göra det.

I svensk rätt döms för *hets mot folkgrupp* (16 kap. 8 § brottsbalken) den som – i 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, trosbekännelse eller sexuell läggning. Straffet är fängelse i högst två år eller, om brottet är ringa, böter. Är brottet grovt döms till fängelse lägst sex månader och högst fyra år. Vid bedömande av om brottet är grovt ska 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. Försök eller förberedelse till hets mot folkgrupp är inte kriminaliserat.

Enligt bestämmelsens ursprungliga lydelse bestod den brottsliga gärningen i hot, förtal eller smädelse. Dessa ord var att förstå enligt gängse språkbruk, och så är också fallet med *hotar* i den nu gällande texten. Uttrycket omfattar således inte endast sådana handlingar som kriminaliserats genom bestämmelserna om olaga hot och olaga tvång. På liknande sätt avses med begreppet *missaktning* inte endast förtal och smädelser utan även andra kränkande omdömen. Inte endast direkta, utan även indirekta, uttryck för missaktning faller inom det straffbara området.[1]

Alla uttalanden av nedsättande eller förnedrande natur omfattas inte. Uttalanden som inte kan anses överskrida gränserna för en saklig kritik av vissa grupper faller utanför det straffbara området. För straffbarhet krävs att det är fullt klart att uttalandet överskrider

[1] I rättsfallet NJA 1982 s. 128 konstaterade Högsta domstolen t.ex. att texten ”Zigenare får ej beträda campingen” på en skylt vid infarten till en campingplats indirekt uttryckte ett omdöme om zigenares egenskaper och uppträdande, som måste anses nedsättande för folkgruppens anseende, varför gärningen bedömdes som hets mot folkgrupp.

gränsen för en saklig och vederhäftig diskussion rörande gruppen i fråga. Hänsyn till opinionsfriheten och kritikrätten får dock inte åberopas som skydd för uttalanden som uttrycker missaktning för en hel folkgrupp på grund av att den t.ex. tillhör en viss nationalitet och av denna anledning skulle vara mindre värd (se prop. 1970:87 s. 130 och 2001/02:59 s. 15).

Med *spridning* avses i bestämmelsen överförande av budskapet till andra personer utanför den helt privata sfären. I den delen fick bestämmelsen sin nuvarande utformning år 1988, då det tidigare kravet på att uttalandet skulle göras offentligen eller spridas bland allmänheten togs bort. Detta innebär att spridning också inom en sammanslutning eller annars till en begränsad krets kan omfattas av straffansvaret (prop. 1986/87:151 s. 110). Spridning kan ske muntligen eller skriftligen men också på annat sätt, t.ex. genom åtbörder eller genom bilder.[2]

De *grupper* som skyddas genom bestämmelsen om hets mot folkgrupp är ”folkgrupp eller annan sådan grupp av personer” när angreppet sker med anspelning på, dvs. tar sin utgångspunkt i, ras, hudfärg, nationellt eller etniskt ursprung, trosbekännelse eller sexuell läggning. Med *ras* menas ”de grupper av människosläktet som brukar upptas i antropologiska rasindelningar” och med folkgrupp av visst *etniskt ursprung* avses ”folkgrupp vari medlemmar har ett relativt enhetligt kulturmönster” (prop. 1970:87 s. 37–38). Enligt förarbetena torde t.ex. samer kunna räknas till den sist nämnda folkgruppen liksom i betydande grad folkgrupper vars medlemmar är av samma nationalitetstillhörighet (prop. 1970:87 s. 38). En folkgrupp torde i det enskilda fallet ofta kunna inordnas under mer än en av de nämnda kategorierna.

Något krav på att hotet eller uttrycket för missaktning direkt avser någon sådan grund som ras, hudfärg etc. ställs inte upp. Även uttalanden som innefattar kränkande beskyllningar om mindervärda egenskaper eller nedsättande handlingar men endast medelbart grundas på exempelvis etniskt ursprung faller under bestämmelsen. Bestämmelsen tar sikte på angrepp som riktas mot kollektivt bestämda grupper och kollektiv av sådana grupper (t.ex. ”befolkningsgruppen invandrare”), något som i lagtexten markeras genom ordvalet ”folkgrupp eller annan sådan grupp av personer”, (se prop. 1981/82:58 s. 44–45). Enskilda identifierbara individer

[2] Exempelvis har Högsta domstolen i NJA 1996 s. 577 slagit fast att bärande av symboler som kan förknippas med nazisternas förföljelse av judar och andra folkgrupper före och under andra världskriget kan utgöra hets mot folkgrupp.

eller grupper av sådana individer, t.ex. en familj som utsätts för förföljelse i ett bostadsområde, skyddas däremot inte av bestämmelsen. Skyddet för enskilda medlemmar av en grupp följer alltså endast indirekt av att gruppen i sin helhet skyddas.[3] Rasistiska angrepp som riktas direkt mot individer på grund av t.ex. deras nationella ursprung kan i stället bestraffas genom andra bestämmelser om bl.a. olaga hot, ofredande eller förolämpning. För straffbarhet krävs inte att någon bestämd folkgrupp eller annan sådan grupp av personer pekas ut. Även allmänna uttalanden, som t.ex. prisar en viss förment ras, exempelvis ”den vita rasen”, på ett sådant sätt att andra förmenta raser måste anses angripna, är straffbara.

Bestämmelsen om hets mot folkgrupp utgör en begränsning av den i regeringsformen grundlagsfästa yttrandefriheten, närmast med hänvisning till allmän ordning och säkerhet. Bestämmelsen tangerar också rätten att ge ut och sprida tryckta skrifter och att i dem uttrycka tankar och åsikter som regleras i tryckfrihetsförordningen (TF), liksom den motsvarande friheten att yttra sig i vissa andra närmare angivna medier, såsom ljudradio, television, filmer, videogram och ljudupptagningar, som regleras i yttrandefrihetsgrundlagen (YGL).

TF innehåller i 7 kap. 4 och 5 §§ en fullständig uppräkning av de gärningar som utgör tryckfrihetsbrott, när de begås genom tryckt skrift och är straffbara enligt vanlig lag. En av dessa gärningar är hets mot folkgrupp (7 kap. 4 § 11). I 5 kap. 1 § första stycket YGL sägs att de gärningar som anges som tryckfrihetsbrott i 7 kap. 4 och 5 §§ TF ska anses som yttrandefrihetsbrott, om de begås i ett radioprogram eller en teknisk upptagning och är straffbara enligt lag.

YGL kan vara tillämplig på sådan spridning som sker via internet på hemsidor knutna till massmedieföretag (se 1 kap. 9 § YGL). Det finns flera rasistiska publikationer som har utgivningsbevis och som tillhandahåller artiklar m.m. på sina hemsidor (se prop. 2001/02:59 s. 29). Dessa hemsidor omfattas då av YGL.[4] Grundlagen kan även vara tillämplig vid t.ex. massutskick av e-post.

När det gäller påföljder för tryck- och yttrandefrihetsbrott hänvisar TF och YGL till brottsbalken.

---

[3] Av detta följer att målsägandetalan inte är möjlig vid brottet hets mot folkgrupp, se NJA 1978 s. 3.

[4] NJA 2007 s. 805 II gällde just hets mot folkgrupp som yttrandefrihetsbrott. I rättsfallet hade Nationalsocialistisk front publicerat två artiklar rörande dels homosexuella, dels romer på sin webbplats. Nationalsocialistisk front hade utgivningsbevis för verksamheten. Den ansvarige utgivaren för webbplatsen åtalades för hets mot folkgrupp enligt 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. Vanliga straffrättsliga regler om ansvar för medverkande tillämpas alltså inte. 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 *formellt* i den meningen att det faller på den i TF respektive YGL utpekade personen oavsett hur han eller hon har bidragit till framställningen eller vad han eller hon har känt till om innehållet i denna.

Såväl TF som YGL gäller främst för sådant som produceras och sprids i Sverige. I viss utsträckning är reglerna även tillämpliga på utländska yttranden (se SOU 2001:28 s. 101–105 för en närmare redogörelse).

För *förtal* (5 kap. 1 § brottsbalken) 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. Straffet är böter. Är brottet att anse som grovt döms för *grovt förtal* (5 kap. 2 § brottsbalken) till böter eller fängelse i högst två år. Vid bedömningen av om brottet är grovt ska 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. 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, ska ansvar för förtal inte utdömas.

Förtal får enligt huvudregeln inte åtalas av annan än målsägande (5 kap. 5 § brottsbalken). Om målsäganden anger brottet till åtal och åtal av särskilda skäl anses påkallat ur allmän synpunkt får åklagare dock åtala för förtal och grovt förtal. Förtal är straffbart också som tryck- respektive yttrandefrihetsbrott (7 kap. 4 § 14 TF och 5 kap. 1 § första stycket YGL).

I svensk rätt döms vidare den för *uppvigling* (16 kap. 5 § brottsbalken) som bl.a. i skrift som sprids eller lämnas ut för spridning eller i annat meddelande till allmänheten uppmanar till eller söker förleda till brottslig gärning (exempelvis hets mot folkgrupp eller våld eller hot med rasistiskt motiv). Uppvigling kan sägas vara en offentlig uppmaning till brott (Berggren m.fl., *Brottsbalken En*

kommentar kap. 13–24, s. 16:19). Försök och förberedelse till uppvigling är inte straffbart. 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 ska inte dömas till ansvar. Vid bedömningen av om det är fråga om ett ringa fall ska särskilt beaktas om det har förelegat endast obetydlig fara för att uppmaningen eller försöket skulle leda till efterföljd. Uppvigling är straffbart också som tryckrespektive yttrandefrihetsbrott (7 kap. 4 § 11 TF och 5 kap. 1 § första stycket YGL).

I lagen (1998:112) om ansvar för 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 (se avsnitt 5.3.10), skyldig att hålla viss 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 ska 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 § första stycket). Om brottet är grovt är straffet fängelse i högst två år. I ringa fall ska inte dömas till ansvar. Straffbestämmelsen är subsidiär till reglerna i brottsbalken (7 § andra stycket).[5]

Tilläggsprotokollets definition av rasistiskt och främlingsfientligt material överensstämmer i stort med hur det straffbara området har avgränsats i bestämmelsen om hets mot folkgrupp. Begreppet ”härstamning” i tilläggsprotokollets definition återfinns emellertid inte i den svenska bestämmelsen. Enligt den förklararande rapporten (p. 19) åsyftas med begreppet inte socialt ursprung, utan det avser främst att omfatta personer eller grupper av personer som härstammar från personer som kan kännas igen genom vissa särdrag, exempelvis hudfärg. Begreppet får därför anses i den svenska bestämmelsen om hets mot folkgrupp täckas av antingen ras, hudfärg eller nationellt eller etniskt ursprung. Tilläggsprotokollet omfattar vidare material som förespråkar, främjar eller uppmuntrar till

[5] I NJA 2007 s. 805 I var fråga om underlåtenhet att ta bort meddelanden från en elektronisk anslagstavla kunde utgöra medhjälp till hets mot folkgrupp eller brott mot lagen om ansvar för elektroniska anslagstavlor.

inte bara *hot* eller *våld* (jfr *hotar* i bestämmelsen om hets mot folkgrupp) utan även *diskriminering*. Att förespråka, främja eller uppmuntra diskriminering torde täckas av begreppet *uttrycka missaktning* enligt bestämmelsen om hets mot folkgrupp.

Med att *tillgängliggöra* enligt artikel 3 avses även sådana åtgärder som att skapa eller sammanställa länkar. Som framgått har spridningsrekvisitet i bestämmelsen om hets mot folkgrupp i praxis tolkats relativt extensivt och som spridning i bestämmelsens mening även ansetts exempelvis att bära vissa symboler. Vår mening är därför att det kan förmodas att även en sådan åtgärd som skapande av länkar skulle kunna anses som spridning enligt bestämmelsen om hets mot folkgrupp.

Vår uppfattning är att de gärningar som enligt artikel 3 ska straffbeläggas i huvudsak täcks av bestämmelsen om hets mot folkgrupp.

Som rasistiskt och främlingsfientligt material avses emellertid enligt tilläggsprotokollet även material som förespråkar, främjar eller uppmuntrar till hat, diskriminering eller våld mot *en enskild person*. Skyddsobjektet i bestämmelsen om hets mot folkgrupp är dock, som framgått, *kollektivt bestämda grupper* och *kollektiv av sådana grupper*. Att sprida material som exempelvis uppmuntrar till våld mot en enskild utpekad person på grund av dennes hudfärg kan i svensk rätt, i stället för hets mot folkgrupp, vara att bedöma som uppvigling. Ett rasistiskt motiv ska beaktas som en försvårande omständighet vid bedömningen av straffvärdet enligt den allmänna straffskärpningsregeln i 29 kap. 2 § 7 brottsbalken, varvid även denna då kan tillämpas. Gärningen skulle också i vissa fall, beroende på omständigheterna, kunna vara att bedöma som förtal.

Sammanfattningsvis är det vår bedömning att svensk rätt, genom främst bestämmelserna om hets mot folkgrupp och uppvigling, uppfyller konventionens krav på vad som ska vara straffbelagt som spridande av rasistiskt och främlingsfientligt material med hjälp av datorsystem.

Som framgått är såväl hets mot folkgrupp som uppvigling (och förtal) straffbart också som tryck- respektive yttrandefrihetsbrott. Det finns alltså möjlighet att ingripa mot gärningar som artikel 3 avser att straffbelägga, även när dessa begås i ett grundlagsskyddat medium. Vi återkommer i avsnitt 6.2.6 till frågan om den särskilda ansvarsordningen i TF och YGL bör föranleda något svenskt förbehåll.

6.2.3 Rasistiskt och främlingsfientligt motiverat hot (artikel 4)

Bedömning: Svensk rätt uppfyller genom bestämmelserna om olaga hot och hets mot folkgrupp tilläggsprotokollets krav på vad som ska vara straffbelagt som rasistiskt och främlingsfientligt motiverat hot.

Skälen för bedömningen

Enligt *artikel 4* ska det vara straffbart att uppsåtligen och orättmätigt med hjälp av ett datorsystem hota

- 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
- en grupp av personer som utmärks av något av de karakteristika som nämnts i den föregående punkten,

med att begå brott som i den fördragsslutande statens nationella lagstiftning definieras som allvarliga.

Det hot som avses i artikeln behöver inte ha uttryckts offentligt (se den förklarande rapporten p. 35). Det är, som uttryckligen framgår av artikeln, en sak för varje fördragsslutande stat att avgöra vad som är att anse som ett allvarligt brott (se även den förklarande rapporten p. 34). Tilläggsprotokollet kräver inte att hot som är rasistiskt och främlingsfientligt motiverade straffbeläggs särskilt i den nationella rätten, utan det är tillräckligt att hot i allmänhet är straffbelagt (se den förklarande rapporten p. 33).

I svensk rätt är det främst bestämmelserna om *olaga hot* och *hets mot folkgrupp* som motsvarar de gärningar som artikel 4 avser att straffbelägga. För en redogörelse över brottet hets mot folkgrupp, se avsnitt 6.2.2.

För *olaga hot* (4 kap. 5 § brottsbalken) döms den som lyfter vapen mot annan eller på annat sätt hotar med brottslig gärning på sätt som är ägnat att hos den hotade framkalla allvarlig fruktan för egen eller annans säkerhet till person eller egendom. Hotet behöver inte uttryckas offentligt men det förutsätts att hotet ska ha kommit till den hotades kännedom. Motiven för hotet saknar betydelse för

straffansvar. Ett rasistiskt motiv ska dock beaktas som en försvårande omständighet vid bedömningen av straffvärdet enligt den allmänna straffskärpningsregeln i 29 kap. 2 § 7 brottsbalken. 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. Olaga hot är straffbart också som tryck- respektive yttrandefrihetsbrott (7 kap. 4 § 16 TF och 5 kap. 1 § första stycket YGL).

Vår bedömning är att de svenska bestämmelserna om olaga hot och hets mot folkgrupp uppfyller tilläggsprotokollets krav på vad som ska vara straffbart som rasistiskt och främlingsfientligt motiverat hot.

Olaga hot och hets mot folkgrupp kan som framgått även bestraffas som tryck- och yttrandefrihetsbrott. Brott som avses i artikel 4 kan alltså i svensk rätt beivras trots att de begås i ett grundlagsskyddat medium. Vi återkommer i avsnitt 6.2.6 till betydelsen av den särskilda ansvarsordningen i TF och YGL.

6.2.4 Rasistiskt och främlingsfientligt motiverad kränkning (artikel 5)

Bedömning: Svensk rätt uppfyller genom bestämmelserna om hets mot folkgrupp och förtal tilläggsprotokollets krav på vad som ska vara straffbelagt som rasistiskt och främlingsfientligt motiverad kränkning. Något behov av att för svensk del uppställa krav på att brotten ska resultera i att den person eller de grupper av personer som utsätts för kränkning också utsätts för hat, missaktning eller löje finns inte.

Skälen för bedömningen

Enligt *artikel 5.1* ska det vara straffbart att uppsåtligen och orättmätigt, med hjälp av ett datorsystem, offentligen kränka

- 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
- en grupp personer som utmärks av de karakteristika som nämnts i den föregående punkten.

Av *artikel 5.2* framgår att en fördragsslutande stat får uppställa krav på att det brott som avses i artikel 5.1 resulterar i att personen eller gruppen av personer utsätts för hat, missaktning eller löje. Vidare framgår att en fördragsslutande stat får förbehålla sig en möjlighet att helt eller delvis inte straffbelägga de gärningar som avses i artikel 5.1.

Till skillnad från hot enligt artikel 4, vilka som framgått kan ha uttryckts enbart inom ramen för den personliga sfären, ska det kränkande uttalandet enligt artikel 5 ha uttryckts offentligt (se den förklarande rapporten p. 36).

I svensk rätt är det främst bestämmelserna om *hets mot folkgrupp* och *förtal* som motsvarar de gärningar som artikel 5 avser att straffbelägga (se närmare om brotten i avsnitt 6.2.2). Av den närmare beskrivningen av brottet hets mot folkgrupp i avsnitt 6.2.2 framgår att uttrycket *hotar* är att förstå enligt gängse språkbruk och därför inte endast omfattar sådana handlingar som kriminaliserats genom bestämmelserna om olaga hot och olaga tvång, och vidare att med begreppet *missaktning* inte avses endast förtal och smädelser utan även andra kränkande omdömen samt att inte endast direkta, utan även indirekta, uttryck för missaktning faller inom det straffbara området. Bestämmelsen om hets mot folkgrupp täcker således i huvudsak det område som artikel 5 avser att kriminalisera.

Skyddsobjektet i bestämmelsen om hets mot folkgrupp är dock, som angetts i avsnitt 6.2.2, *kollektivt bestämda grupper* och *kollektiv av sådana grupper*. Kränkande offentliga omdömen som riktar sig mot en enskild identifierbar individ träffas alltså inte av bestämmelsen. Sådana omdömen kan dock enligt svensk rätt utgöra förtal.

För *förolämpning* (5 kap. 3 § brottsbalken), döms den som smädar annan genom kränkande tillmäle eller beskyllning eller genom något annat skymfligt beteende mot honom, om gärningen inte är belagd med straff för förtal eller grovt förtal.[6] Det utmärkande för brottet är, till skillnad mot förtalsbrottet, att uttalandet ska rikta sig till den person som berörs av det. Ett uttalande till tredje man är därför inte att bedöma som förolämpning utan är straffritt, om det inte innebär förtal (jfr Berggren m.fl., *Brottsbalken En kommentar kap. 1–12*, s. 5:26). Bestämmelsen torde därför inte ha någon nämnvärd betydelse för frågan om svensk rätt uppfyller artikel 5, eftersom denna artikel tar sikte på offentliga uttalanden.

[6] När det specifikt gäller rasistiska uttalanden, kan nämnas att i NJA 1989 s. 374 dömdes en man som kallat en kvinna av främmande etniskt ursprung för ”jävla svartskalle” för förolämpning. Uttalandet ansågs ha syftat till och varit ägnat att kränka kvinnans självkänsla.

Vår bedömning är att svensk rätt genom bestämmelserna om hets mot folkgrupp och förtal uppfyller tilläggsprotokollets krav på vad som ska vara straffbelagt som rasistiskt och främlingsfientligt motiverad kränkning. Något behov av att för svensk del uppställa krav på att brotten enligt artikeln ska resultera i att den person eller de grupper av personer som utsätts för kränkningen också utsätts för hat, missaktning eller löje finns inte. Varken i bestämmelsen om hets mot folkgrupp eller i förtalsbestämmelsen uppställs något sådant krav för fullbordat brott.

Som framgått i avsnitt 6.2.2, är såväl hets mot folkgrupp som förtal straffbart också som tryck- respektive yttrandefrihetsbrott. Det finns alltså möjlighet att ingripa mot gärningar som artikel 5 avser att straffbelägga, även när dessa begås i ett grundlagsskyddat medium. Vi återkommer i avsnitt 6.2.6 till frågan om den särskilda ansvarsordningen i TF och YGL bör föranleda något svenskt förbehåll.

6.2.5 Förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten (artikel 6)

Bedömning: Svensk rätt uppfyller genom främst bestämmelserna om hets mot folkgrupp och uppvigling tilläggsprotokollets krav på vad som ska vara straffbelagt som förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten, om krav uppställs på att förnekandet eller det grova förringandet 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.

Skälen för bedömningen

I *artikel 6.1* uppställs krav på kriminalisering av gärningar som innebär att någon uppsåtligen och orättmätigt med hjälp av ett datorsystem sprider eller på annat sätt för allmänheten tillgängliggör material som förnekar, grovt förringar, gillar eller rättfärdigar gärningar som enligt folkrätten eller vissa internationella domstolar utgör folkmord eller brott mot mänskligheten.

Av *artikel 6.2 a* framgår att en fördragsslutande stat får uppställa krav på att förnekandet eller det grova förringande som avses i artikel 6.1 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.

Enligt *artikel 6.2 b* får en fördragsslutande stat förbehålla sig en möjlighet att helt eller delvis inte straffbelägga de gärningar som avses i artikel 6.1.

I svensk rätt finns inte någon straffbestämmelse som helt motsvarar de gärningar som artikel 6.1 avser att kriminalisera. Anledningen till detta är främst att hänföra till den i regeringsformen (2 kap. 1 § 1) grundlagsfästa yttrandefriheten. För att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, bl.a. med hänsyn till allmän ordning och säkerhet, tillåter regeringsformen emellertid att yttrandefriheten begränsas i lag (2 kap. 20 § 1, 21 och 22 §§).

Som framgått i avsnitt 6.2.2, utgör bestämmelsen om hets mot folkgrupp en begränsning av den grundlagsfästa yttrandefriheten. Bestämmelsen innebär ett relativt stort ingrepp i yttrandefriheten. Regeringen har, syftande på bestämmelsen, uttalat att hänsyn till opinionsfriheten och kritikrätten inte får åberopas som skydd för uttalanden som uttrycker missaktning för en hel folkgrupp på grund av att den t.ex. tillhör en viss nationalitet och av denna anledning skulle vara mindre värd (prop. 1970:87 s. 130 och 2001/02:59 s. 15). I svensk rätt är det emellertid inte straffbart att exempelvis ge till känna en åsikt om ett visst historiskt skede, såsom förintelsen, även om det är uppenbart att åsikten i fråga är felaktig i sak och är av sådant slag att samhället i stort tar avstånd från den. Vi anser inte att det är aktuellt att inom ramen för vårt uppdrag föreslå några ändringar som ytterligare begränsar yttrandefriheten, om alternativ till detta finns.

De gärningar som artikel 6.1 avser att straffbelägga torde i många fall utgöra hets mot folkgrupp i svensk rätt (för en närmare redogörelse för bestämmelsen om hets mot folkgrupp, se avsnitt 6.2.2; jfr särskilt NJA 1996 s. 577). Skyddsobjektet i bestämmelsen om hets mot folkgrupp är emellertid kollektivt bestämda grupper och för straffansvar förutsätts att det meddelande som sprids ger uttryck för hot eller missaktning med anspelning på ras, hudfärg etc. Vid en jämförelse mellan artikel 6 och bestämmelsen om hets mot

folkgrupp kan följande slutsats dras. För det fall krav uppställs på att förnekandet eller det grova förringandet som avses i punkten 1 görs med sådant uppsåt som nämns i punkten 2 a (uppsåt att uppmuntra till hat, diskriminering eller våld) mot en grupp av personer på grund av ras, hudfärg, härstamning etc. uppfyller svensk rätt genom bestämmelsen om hets mot folkgrupp det som artikeln avser att kriminalisera när det gäller *grupper av personer*. Som vi redovisat i avsnitt 6.2.2 är vår bedömning att spridningsbegreppet i bestämmelsen om hets mot folkgrupp omfattar sådana åtgärder som avses med det i tilläggsprotokollet använda begreppet ”för allmänheten göra tillgängligt”.

När det gäller *enskilda identifierbara personer* skyddas de, som framgått av avsnitt 6.2.2, i de sammanhang som nu avses inte av bestämmelsen om hets mot folkgrupp utan främst av bestämmelsen om uppvigling. Ansvar för förtal kan även komma i fråga och eventuellt skulle även ansvar för olaga hot i vissa fall kunna bli aktuellt. Om krav, på samma sätt som föreslagits när det gäller grupper av personer, uppställs på att förnekandet eller det grova förringandet som avses i punkten 1 görs med uppsåt att uppmuntra till hat, diskriminering eller våld mot en enskild person är det svårt att tänka sig en situation i vilken gärningen i svensk rätt skulle vara straffri. Ansvar för exempelvis uppvigling eller olaga hot torde därvid kunna komma i fråga.

Sammanfattningsvis gör vi således bedömningen att svensk rätt genom främst bestämmelserna om hets mot folkgrupp och uppvigling uppfyller protokollsåtagandet när det gäller förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten, om krav enligt punkten 2 a uppställs på att förnekandet eller det grova förringandet 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. Möjligheten till förbehåll enligt punkten 2 b behöver alltså då inte utnyttjas.

I sammanhanget kan erinras om att i EU:s rambeslut om bekämpande av vissa former av och uttryck för rasism och främlingsfientlighet enligt strafflagstiftningen, finns vissa med artikel 6 parallella bestämmelser. Enligt rambeslutets artikel 1 ska varje medlemsstat vidta de åtgärder som är nödvändiga för att se till att vissa uppräknade avsiktliga gärningar blir straffbara. Som sådana gärningar anges i artikelns punkt 1 c och d:

c) Offentligt urskuldande, förnekande eller flagrant förringande av brott som folkmord, brott mot mänskligheten och krigsförbrytelser enligt definitionen i artiklarna 6, 7 och 8 i Internationella brottmålsdomstolens stadga, riktat mot en grupp av personer eller en medlem av en sådan grupp, utpekad med åberopande av ras, hudfärg, religion, härstamning eller nationellt eller etniskt ursprung, om gärningen begås på ett sådant sätt att den är ägnad att uppmana till våld eller hat gentemot en sådan grupp eller en medlem av en sådan grupp.

d) Offentligt urskuldande, förnekande eller flagrant förringande av de brott som definieras i artikel 6 i Internationella militärtribunalens stadga, som fogas till Londonöverenskommelsen av den 8 augusti 1945, riktat mot en grupp av personer eller en medlem av en sådan grupp, utpekad med åberopande av ras, hudfärg, religion, härstamning eller nationellt eller etniskt ursprung, om gärningen begås på ett sådant sätt att den är ägnad att uppmana till våld eller hat gentemot en sådan grupp eller en medlem av en sådan grupp.

Artikeln ger (enligt punkt 2) medlemsstaterna en möjlighet att vid tillämpningen välja att straffa enbart gärningar som begås på ett sådant sätt att de är ägnade att vara störande för allmän ordning eller som är hotfulla, otillbörliga eller kränkande.

Som angetts i avsnitt 6.2.1 har regeringen gjort bedömningen att svensk rätt uppfyller rambeslutets krav (Ju2008/3200/L5). Vid bedömningen har angetts att straffbestämmelserna i brottsbalken om olaga hot, uppvigling och hets mot folkgrupp omfattar de förfaranden som enligt artikel 1.1 ska vara kriminaliserade. Vid bedömningen att svensk lag motsvarar åtagandet i artikel 1.1 c och d har Sverige valt att, med stöd av artikel 1.2, straffa enbart gärningar som antingen begås på ett sådant sätt att de är ägnade att vara störande för allmän ordning eller som är hotfulla, otillbörliga eller kränkande.

Som framgått i avsnitt 6.2.2, är såväl hets mot folkgrupp som uppvigling straffbart också som tryck- respektive yttrandefrihetsbrott. Vi återkommer i avsnitt 6.2.6 till frågan om den särskilda ansvarsordningen i TF och YGL bör föranleda något svenskt förbehåll.

6.2.6 Förbehåll i anledning av tryckfrihetsförordningens och yttrandefrihetsgrundlagens särskilda ansvarsordning?

Bedömning: Sverige behöver inte göra några särskilda förbehåll enligt tilläggsprotokollets straffrättsliga artiklar i anledning av den särskilda ansvarsordning som gäller för tryck- och yttrandefrihetsbrott.

Skälen för bedömningen

Vi har i avsnitt 6.2.2–6.2.5 gjort bedömningen att svensk rätt uppfyller tilläggsprotokollets krav på straffbeläggande av brotten i artiklarna 3–6, under förutsättning av att Sverige uppställer krav av visst slag såvitt avser artikel 6. Som redogjorts för i de nämnda avsnitten kan de brott som vi ansett motsvara de gärningar som ska straffbeläggas enligt tilläggsprotokollet i vissa fall i svensk rätt vara att bedöma som tryck- eller yttrandefrihetsbrott. Av avsnitt 6.2.2 har framgått att för brott enligt TF och YGL gäller en särskild ansvarsordning. Principen om ensamansvar innebär att endast en av de oftast många personer som medverkat vid tillkomsten av en framställning med grundlagsskydd enligt TF eller YGL kan hållas straffrättsligt ansvarig för innehållet i framställningen och att det i dessa grundlagar anges vem denna person är. Ansvaret enligt TF och YGL för innehållet i en framställning kallas till följd härav exklusivt. Ansvaret är också successivt vilket betyder att det i första hand åvilar den som kan sägas stå närmast brottet och om ansvaret inte kan utkrävas av denne åvilar det den som står närmast honom eller henne i ansvarskedjan. Slutligen är ansvaret även formellt i den meningen att det åvilar den i TF eller YGL angivne oavsett hur hon eller han bidragit till framställningens tillkomst och oavsett om hon eller han faktiskt känt till dess innehåll.

I promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6) gjordes bedömningen att förbehåll för etablerade principer om yttrandefrihet var nödvändigt enligt artikel 3.3, 5.2 b och 6.2 b för att garantera den svenska särregleringen av tryck- och yttrandefrihetsbrott även i framtiden (Ds 2005:6 s. 352–353).

I tilläggsprotokollets ingress anges, som nämnts i bl.a. avsnitt 6.2.1, generellt att protokollet inte är avsett att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem. I artikel 3.3 finns vidare en möjlighet för en fördragsslutande stat att förbehålla

sig en möjlighet att inte straffbelägga vissa gärningar som avses i artikeln, under hänvisning till etablerade principer om yttrandefrihet i statens rättssystem. Den sist nämnda möjligheten till förbehåll under hänvisning till yttrandefriheten tar emellertid sikte på en möjlighet att *underlåta kriminalisering*. Den frågeställning som nu behandlas avser emellertid något annat, eftersom de aktuella gärningarna *är kriminaliserade* i svensk rätt, men för dem gäller en speciell ansvarsordning.

Samtliga de brott som vi i svensk rätt ansett motsvara de brott som ska straffbeläggas enligt tilläggsprotokollet är straffbara även som tryck- respektive yttrandefrihetsbrott. Det finns därmed möjlighet att ingripa mot de gärningar som avses i tilläggsprotokollet, även när dessa begås i ett grundlagsskyddat medium. Att den svenska regleringen innebär begränsningar i fråga om vem som kan göras ansvarig för brottet innebär enligt vår mening inte att denna står i konflikt med tilläggsprotokollets krav på kriminalisering, speciellt mot bakgrund av ingresstexten avseende etablerade principer om yttrandefrihet i nationella rättssystem. Mot den bakgrunden är det vår bedömning att, för det fall den gärning som en viss artikel i tilläggsprotokollet avser att kriminalisera är straffbelagd i svensk rätt, såväl som allmänt brott som tryck- respektive yttrandefrihetsbrott, behöver Sverige inte göra något särskilt förbehåll vad gäller den speciella ansvarsordningen för tryck- och yttrandefrihetsbrott. Att straffansvaret åvilar en speciellt utpekad person när det är fråga om tryck- eller yttrandefrihetsbrott är således irrelevant i sammanhanget.

6.2.7 Medhjälp (artikel 7)

Bedömning: Svensk rätt uppfyller tilläggsprotokollets krav på kriminalisering av medhjälp till brotten i tilläggsprotokollet.

Skälen för bedömningen

Enligt *artikel 7* ska uppsåtlig medhjälp till samtliga brott i tilläggsprotokollet vara straffbart.

Som redogjorts för i avsnitt 5.3.12, ådöms i svensk rätt, enligt den allmänna medverkansbestämmelsen i 23 kap. 4 § brottsbalken, straffansvar inte bara den som utfört gärningen utan även annan

som har främjat denna med råd eller dåd. Regeln gäller vid alla brottsbalksbrott samt de brott i specialstraffrätten för vilka fängelse är föreskrivet eller för vilka särskild föreskrift finns att medverkan ska bestraffas.

Den som inte är att anse som gärningsman döms för anstiftan om han eller hon har förmått annan att utföra brottet. I övriga fall döms för medhjälp till brottet. Varje medverkande ska bedömas efter det uppsåt eller den oaktsamhet som han eller hon har visat.

I svensk rätt är anstiftan av och medhjälp till samtliga de brott som vi i avsnitt 6.2.2–6.2.5 ansett motsvara de brott som upptas i artiklarna 3–6 straffbart. Som framgått i de nämnda avsnitten kan brotten emellertid i vissa fall i svensk rätt vara att bedöma som tryck- eller yttrandefrihetsbrott. Som vidare framgått (se avsnitt 6.2.2) innebär principen om ensamansvar i TF och YGL att vanliga straffrättsliga regler om ansvar för medverkande inte tillämpas vid tryck- eller yttrandefrihetsbrott. Mot bakgrund av tilläggsprotokollets ingresstext, i vilken anges att protokollet inte avser att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem, gör vi bedömningen att denna svenska särreglering inte står i konflikt med tilläggsprotokollets krav på ansvar för medhjälp.

6.2.8 Juridiska personers ansvar samt påföljder och åtgärder (del av artikel 8.1)

Bedömning: Svensk rätt får anses uppfylla de krav som tilläggsprotokollet ställer i fråga om dels ansvar för juridiska personer, dels påföljder och åtgärder.

Skälen för bedömningen

Enligt *artikel 8.1* ska vissa av konventionens artiklar, däribland *artikel 12* som gäller juridiska personers ansvar och *artikel 13* som gäller påföljder och åtgärder, i tillämpliga delar gälla även för tilläggsprotokollet.

När det gäller juridiska personers ansvar har vi i avsnitt 5.3.13 gjort bedömningen att svensk rätt genom bestämmelserna om företagsbot och förverkande får anses uppfylla de krav på sanktioner mot juridiska personer som konventionen ställer. Vi gör motsvar-

ande bedömning för tilläggsprotokollets del. Att det för tryck- och yttrandefrihetsbrott gäller särskilda ansvarsregler bedöms, mot bakgrund av tilläggsprotokollets ingresstext angående etablerade principer om yttrandefrihet, i sammanhanget sakna betydelse.

Även när det gäller påföljder och åtgärder har vi gjort bedömningen att svensk rätt uppfyller konventionens krav (se avsnitt 5.3.14). De straffskalor som gäller för de brott som i svensk rätt är av relevans för tilläggsprotokollets del har redovisats i avsnitt 6.2.2–6.2.5. Samtliga dessa, utom förtal av normalgraden, har fängelse i straffskalan. Mot den bakgrunden gör vi bedömningen att svensk rätt även uppfyller tilläggsprotokollets krav i denna del. I sammanhanget bör även erinras om den tidigare nämnda (se bl.a. avsnitt 6.2.3) allmänna straffskärpningsregeln i 29 kap. 2 § 7 brottsbalken som innebär att bl.a. rasistiska eller diskriminerande motiv kan utgöra grund för straffskärpning. I bestämmelsen anges att domstolarna vid straffmätningen ska ta hänsyn till om motivet för brottet varit att kränka en person, en folkgrupp eller annan sådan grupp av personer på grund av ras, hudfärg, nationellt eller etniskt ursprung, trosbekännelse, sexuell läggning eller annan liknande omständighet.

Som framgått i avsnitt 6.2.2 är förtal och grovt förtal som huvudregel målsägandebrott. Detta innebär enligt vår mening inte något problem i förhållande till tilläggsprotokollet, eftersom dels den avsedda gärningen är straffbelagd i svensk rätt, dels allmänt åtal under vissa förutsättningar får ske; målsäganden ska (om denne är över arton år) ange brottet till åtal och åtal ska av särskilda skäl anses påkallat ur allmän synpunkt. Förtal mot någon av rasistiska motiv kan inte sällan tänkas innebära att åtal anses påkallat ur allmän synpunkt.

6.3 Processrättsliga bestämmelser (del av artikel 8.2)

Bedömning: För att tillgodose de krav som följer av tilläggsprotokollet i fråga om processrättsliga regler, krävs inga ytterligare lagändringar än de som följer av konventionens processrättsliga bestämmelser.

Skälen för bedömningen

Enligt *artikel 8.2* ska de fördragsslutande staterna utvidga tillämpningsområdet för bl.a. de åtgärder som anges i konventionens samtliga processrättsliga artiklar till de gärningar som ska straffbeläggas enligt tilläggsprotokollet.

När det gäller krav på processrättsliga regler hänvisar alltså tilläggsprotokollet helt till konventionens processrättsliga bestämmelser. De befogenheter och förfaranden som föreskrivs i konventionens processrättsliga artiklar ska kunna tillämpas på de brott som straffbeläggs i enlighet med tilläggsprotokollet och samma möjligheter till förbehåll som finns enligt konventionen finns enligt tilläggsprotokollet.

Vi har i avsnitt 5.4 med utgångspunkt i konventionens processrättsliga artiklar analyserat vilket behov av lagändring dessa föranleder. De svenska tvångsåtgärder och andra åtgärder som där beskrivs, kan tillämpas även i förhållande till de brott som upptas i tilläggsprotokollet. I den utsträckning den bedömningen har gjorts att konventionens processrättsliga reglering kräver lagändring är detta av relevans även för tilläggsprotokollets del. Några ytterligare lagändringar än de som följer av anpassningen till konventionens processrättsliga artiklar krävs inte mot bakgrund av tilläggsprotokollet. Det förhållandet att vissa av brotten i protokollet i svensk rätt kan vara att bedöma som tryck- eller yttrandefrihetsbrott utgör, mot bakgrund av tilläggsprotokollets ingresstext angående etablerade principer om yttrandefrihet, enligt vår bedömning inte något problem.

Vår bedömning är således att det för att tillgodose de krav som följer av tilläggsprotokollet i fråga om processrättsliga regler inte krävs några ytterligare lagändringar än de som följer av konventionens processrättsliga bestämmelser.

6.4 Domsrätt (del av artikel 8.1)

Bedömning: De allmänna svenska domsrättsreglerna i 2 kap. brottsbalken uppfyller kraven enligt tilläggsprotokollet. Det finns inte någon anledning för Sverige att göra förbehåll om inskränkning av domsrätt enligt artikel 12.2.

Skälen för bedömningen

Enligt *artikel 8.1* ska vissa av konventionens artiklar, däribland, *artikel 22* som gäller domsrätt, i tillämpliga delar gälla även för tilläggsprotokollet.

Vi har i avsnitt 5.5 gjort bedömningen att de allmänna svenska domsrättsreglerna i 2 kap. brottsbalken uppfyller de krav som följer av konventionen i fråga om domsrätt.

För samtliga de brott som i svensk rätt motsvarar brotten i artiklarna 2–7 i tilläggsprotokollet, utom förtal av normalgraden, kan följa svårare straff än böter. Mot den bakgrunden finns inte skäl att göra någon annan bedömning av frågan om svensk rätts förenlighet med tilläggsprotokollets regler om domsrätt än som gjorts vad avser motsvarande regler i konventionen. Som nämnts i tidigare avsnitt anges i tilläggsprotokollets ingresstext att protokollet inte är avsett att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem. Något skäl att i sammanhanget problematisera det förhållandet att vissa av brotten i tilläggsprotokollet i svensk rätt kan vara att bedöma som tryck- eller yttrandefrihetsbrott anser vi mot den bakgrunden inte finnas.

Av artikel 12.2 framgår att en fördragsslutande stat vid tillträdet till tilläggsprotokollet har möjlighet att göra förbehåll enligt konventionens artikel 22.2 (innebärande en inskränkning av konventionens huvudregel om domsrätt), även om något sådant förbehåll inte lämnats i förhållande till konventionen. För svenskt vidkommande finns inte behov av att göra något sådant förbehåll.

6.5 Bestämmelser om internationellt samarbete (del av artikel 8.2)

Bedömning: För att tillgodose de krav som följer av tilläggsprotokollet i fråga om regler för internationellt samarbete, krävs inga ytterligare lagändringar än de som följer av konventionens bestämmelser om internationellt samarbete.

Skälen för bedömningen

Enligt *artikel 8.2* ska de fördragsslutande staterna utvidga tillämpningsområdet för bl.a. de åtgärder som anges i konventionens samtliga bestämmelser om internationellt samarbete till de gärningar som ska straffbeläggas enligt tilläggsprotokollet.

När det gäller krav på regler om internationellt samarbete hänvisar alltså tilläggsprotokollet, på samma sätt som när det gäller processrättsliga regler, helt till konventionens bestämmelser. De grundläggande principer för internationellt samarbete som föreskrivs i konventionen och de särskilda åtgärder som enligt konventionen ska kunna vidtas inom ramen för detta samarbete, ska således kunna tillämpas på brott som straffbeläggs i enlighet med tilläggsprotokollet. Samma möjligheter till förbehåll som finns enligt konventionen finns vidare enligt tilläggsprotokollet.

Vi har i avsnitt 5.6 med utgångspunkt i konventionens artiklar om internationellt samarbete analyserat vilket behov av lagändring dessa föranleder. De svenska bestämmelser om olika former av rättslig hjälp som där beskrivs, kan tillämpas även i förhållande till de brott som upptas i tilläggsprotokollet. I den utsträckning den bedömningen har gjorts att konventionens bestämmelser om rättslig hjälp kräver lagändring är detta av relevans även för tilläggsprotokollets del. Några ytterligare lagändringar än de som följer av anpassningen till konventionens artiklar om internationellt samarbete krävs inte mot bakgrund av tilläggsprotokollet. Det förhållandet att vissa av brotten i protokollet i svensk rätt kan vara att bedöma som tryck- eller yttrandefrihetsbrott utgör, mot bakgrund av tilläggsprotokollets ingresstext angående etablerade principer om yttrandefrihet, enligt vår bedömning inte något problem.[7]

Vår bedömning är således att det för att tillgodose de krav som följer av tilläggsprotokollet i fråga om regler för internationellt samarbete inte krävs några ytterligare lagändringar än de som följer av konventionens bestämmelser om internationellt samarbete.

[7] När det gäller frågan om att lämna internationellt rättsligt bistånd på grundlagsområdet har Yttrandefrihetskommittén i sitt slutbetänkande *En översyn av tryck- och yttrandefriheten* (SOU 2012: 55) föreslagit en ny bestämmelse i TF och YGL. Bestämmelsen innebär att sådant bistånd kan lämnas avseende åtgärder som är tillåtna enligt grundlagarna (se närmare SOU 2012:55, Del 1, s. 506–511). Kommittén har vidare föreslagit att det territoriella tillämpningsområdet för TF och YGL ska minskas genom att det i grundlagarna anges att en här framställd skrift eller teknisk upptagning inte anses utgiven i Sverige enbart på den grunden att den har skickats till enskilda adressater i utlandet (se närmare SOU 2012:55, Del 1 s. 500–505). Yttrandefrihetskommitténs förslag bereds för närvarande i Regeringskansliet.

6.6 Slutbestämmelser (del av artikel 8.1 samt artiklarna 9–16)

Bedömning: Slutbestämmelserna föranleder inte några lagändringar eller specificeringar.

Skälen för bedömningen

Enligt *artikel 8.1* ska vissa av konventionens slutbestämmelser (artikel 41 samt artiklarna 44–46) i tillämpliga delar gälla tilläggsprotokollet. Behovet av lagändringar mot bakgrund av konventionens slutbestämmelser har analyserats i avsnitt 5.7.

Artikel 41 i konventionen rör federala stater.

Enligt *artikel 44* i konventionen kan varje fördragsslutande stat föreslå ändringar av konventionen. Ändringsförslag ska senare enligt en viss procedur underställas de fördragsslutande staterna för antagande.

Av *artikel 45* i konventionen följer att de fördragsslutande staterna ska söka lösa tvister om tolkningen eller tillämpningen av konventionen genom förhandling eller med andra fredliga medel, varvid det särskilt hänvisas till hänskjutande till Europarådets kommitté för brottsfrågor (CDPC), till skiljedomstol eller till Internationella domstolen.

I *artikel 46* i konventionen 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.

Förslag till ändringar av tilläggsprotokollet, tvister om tolkningen eller tillämpningen av protokollet samt frågor om samråd med anledning av genomförande och tillämpning av protokollet etc. ska alltså lösas på samma sätt som när det gäller motsvarande frågor hänförliga till konventionen. Hänvisningen i artikel 8.1 till dessa av konventionens slutbestämmelser föranleder inget behov av lagändringar.

Artikel 9 behandlar frågor om undertecknande. Protokollet står öppet för undertecknande av de stater som har undertecknat kon-

ventionen. En stat kan inte tillträda tilläggsprotokollet innan den tillträtt konventionen.

I *artikel 10* behandlas frågor om ikraftträdande. Som tidigare nämnts trädde tilläggsprotokollet i kraft den 1 mars 2006. I relation till en enskild signatärstat träder tilläggsprotokollet i kraft första dagen i den månad som följer efter utgången av en period på tre månader efter den dag då signatären uttryckt sitt samtycke till att vara bunden av protokollet.

Artikel 11 gäller stater som har anslutit sig till konventionen men som inte är medlemmar i Europarådet eller har deltagit i konventionens utarbetande (jfr artikel 37 i konventionen). Enligt artikeln får en sådan stat även ansluta sig till tilläggsprotokollet sedan detta har trätt i kraft.

Enligt *artikel 12* gäller förbehåll och förklaringar som en stat har avgett rörande bestämmelser i konventionen också för tilläggsprotokollet, om inte staten förklarar något annat. Där anges vidare i vilken utsträckning de fördragsslutande staterna får förklara att de utnyttjar möjligheten att ställa upp särskilda rekvisit, nämligen i fråga om artiklarna 3, 5 och 6 i protokollet. Vidare anges att en fördragsslutande stat, med avseende på bestämmelserna i protokollet, har möjlighet att göra förbehåll enligt två artiklar i konventionen, nämligen artikel 22.2 och artikel 41.1, oavsett eventuella förbehåll som staten har gjort enligt konventionen. Några andra förbehåll är inte tillåtna. Vi har behandlat möjligheterna att göra undantag i anslutning till de bestämmelser i sak där det varit befogat att överväga en förklaring eller ett förbehåll. Vi återkommer i avsnitt 8 till i vilken utsträckning Sverige föreslås utnyttja möjligheten till förbehåll eller förklaringar.

Artikel 13 behandlar återtagande av förbehåll.

I *artikel 14* ges en fördragsslutande stat möjlighet att ange för vilket eller vilka territorier protokollet ska gälla. För svensk del finns inte någon anledning att avge någon sådan specificering.

Enligt *artikel 15* kan en fördragsslutande stat när som helst säga upp protokollet genom ett meddelande ställt till Europarådets generalsekreterare.

Artikel 16, slutligen, anger de meddelanden (om undertecknande, deponering av olika instrument, ikraftträdande osv.) som ska lämnas från Europarådets generalsekreterare till bl.a. de fördragsslutande staterna.

Artiklarna 9–16 innehåller inte något som kräver lagstiftningsåtgärder.

7 Behovet av lagändringar mot bakgrund av direktivet

7.1 Inledning

Syftet med Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF (direktivet) är att ändra och utöka bestämmelserna i rambeslut 2005/222/RIF om angrepp mot informationssystem (rambeslutet). Förhandlingarna om direktivet är i allt väsentligt slutförda. Efter att direktivet antagits har medlemsstaterna två år på sig att genomföra det.

Direktivet bygger på Europarådets konvention om it-relaterad brottslighet (konventionen), som enligt direktivets beaktandesats 8 är den viktigaste rättsliga referensramen när det gäller att bekämpa it-brottslighet, inklusive angrepp mot informationssystem.

Direktivet syftar således till att ytterligare närma medlemsstaternas strafflagstiftning till varandra på området för angrepp mot informationssystem och att inom detta område fastställa minimiregler när det gäller definitionen av vad som ska utgöra brott och vilka påföljder som ska följa på brotten. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna. Eftersom direktivet avser att tillskapa minimiregler och inte att fullharmonisera politikområdet utgör det inte något hinder att ha nationella straffrättsliga regler som går längre än vad direktivet kräver.

Tyngdpunkten i direktivet utgörs av materiella straffrättsliga bestämmelser. Efter artikel 1 och 2 som innehåller en beskrivning av syftet med direktivet och definitioner av vissa begrepp, behandlas i artiklarna 3–7 vilka gärningar som ska utgöra brott, om de utförs uppsåtligen och orättmätigt. Dessa gärningar är olagligt intrång i informationssystem (artikel 3), olaglig systemstörning (artikel 4), olaglig datastörning (artikel 5), olaglig avlyssning (artikel 6)

och vissa åtgärder med verktyg som används för att begå brott (artikel 7). I artikel 8 anges att anstiftan av och medhjälp till sådana gärningar som utgör brott enligt direktivet ska straffbeläggas. Det anges även vilka gärningar som ska straffbeläggas på försöksnivå. Artikel 9 innehåller både generella och artikelspecifika bestämmelser om vilka påföljder som ska kunna dömas ut för brotten i direktivet. Artikel 10 har under förhandlingarna utgått ur utkastet till direktiv. I artiklarna 11 och 12 regleras juridiska personers ansvar samt påföljder för juridiska personer. Jurisdiktionsfrågor regleras i artikel 13. Därefter följer i artikel 14 bestämmelser om informationsutbyte och i artikel 15 bestämmelser om övervakning och statistik. Direktivet avslutas med bestämmelser om ersättande av rambeslutet, införlivande och rapporteringsskyldighet m.m. (artiklarna 16–20).

I vårt uppdrag ingår att analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra direktivet. I det följande analyseras, med utgångspunkt i direktivets artiklar, vilket behov av lagändringar som direktivet föranleder. Den inledande bestämmelsen om syfte (artikel 1), liksom de avslutande bestämmelserna om ersättande av rambeslut, införlivande, rapportering, ikraftträdande och adressater (artiklarna 16–20) är emellertid av sådan generell karaktär att de inte närmare berörs i avsnittet. Vi vill dock framhålla att vår uppfattning är att dessa bestämmelser inte föranleder något särskilt behov av lagstiftningsåtgärder eller andra åtgärder.

Eftersom direktivets bestämmelser, i synnerhet på straffrättens område, till stor del överensstämmer med dem som finns i konventionen är den analys av behovet av lagändringar mot bakgrund av konventionen som vi gjort i avsnitt 5 i många fall av relevans även för frågan om svensk rätt lever upp till direktivets krav. När det gäller flera av direktivets artiklar görs därför i det följande en hänvisning till det avsnitt i vilket vi analyserat behovet av lagändringar mot bakgrund av motsvarande artikel i konventionen.

7.2 Definitioner (artikel 2)

I *artikel 2* ges vissa definitioner som gäller vid tillämpning av direktivet.

Med *informationssystem* i direktivets mening avses en apparat eller en grupp av sammankopplade apparater eller 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 ska kunna drivas, användas, skyddas och underhållas.

Definitionen av informationssystem är densamma som finns i rambeslutet (jfr artikel 1 a i rambeslutet). I konventionen används genomgående begreppet *datorsystem* i stället för informationssystem, men med i huvudsak samma betydelse (jfr artikel 1 a i konventionen).

Med *datorbehandlingsbara uppgifter* i direktivets mening 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.

Definitionen av datorbehandlingsbara uppgifter är densamma som finns i rambeslutet (jfr artikel 1 b i rambeslutet). Konventionens definition av begreppet överensstämmer även det med direktivets, men där används, som nämnts, begreppet datorsystem i stället för informationssystem (jfr artikel 1 b i konventionen).

Med *juridisk person* i direktivets mening avses enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer.

Definitionen av juridisk person är densamma som finns i rambeslutet (jfr artikel 1 c i rambeslutet). Begreppet juridisk person används även i konventionen men definieras inte där närmare.

Med *orättmätigt* i direktivets mening menas intrång, störning, avlyssning eller något annat handlande som avses i direktivet, som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta, eller som inte medges i den nationella lagstiftningen.

Definitionen av orättmätigt är densamma som finns i rambeslutet (jfr artikel 1 d i rambeslutet). Begreppet orättmätigt (”without right”) används i samtliga konventionens straffbestämmelser, men definieras inte särskilt i konventionstexten. Av den förklarande rapporten (p. 38) framgår dock att med begreppet avses i huvudsak detsamma som i direktivet.

7.3 Straffrättsliga bestämmelser

7.3.1 Olagligt intrång i informationssystem (artikel 3)

Bedömning: Svensk rätt uppfyller genom dataintrångsbestämmelsen direktivets krav på vad som ska vara straffbelagt som olagligt intrång i informationssystem.

Skälen för bedömningen

Enligt *artikel 3* ska orättmätigt intrång i hela eller en del av ett informationssystem vara straffbart när brottet begås med uppsåt och genom intrång i en säkerhetsåtgärd. Ringa fall behöver dock inte straffbeläggas.

Bestämmelsen överensstämmer i princip med artikel 2 i rambeslutet. Den motsvarar även i huvudsak artikel 2 om olagligt intrång i konventionen.

Vid genomförandet av rambeslutet konstaterades att svensk rätt genom bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken uppfyllde kravet på vad som ska vara straffbelagt som olagligt intrång i informationssystem (prop. 2006/07:66 s. 22–24).

I avsnitt 5.3.3 har vi gjort bedömningen att svensk rätt genom dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som olagligt intrång. Eftersom direktivets artikel om olagligt intrång i informationssystem i allt väsentligt motsvarar konventionens artikel om olagligt intrång är analysen i avsnittet av relevans även för frågan om svensk rätt lever upp till direktivets krav i denna del. Vi hänvisar därför till denna analys.

Mot den angivna bakgrunden är vår bedömning att svensk rätt genom dataintrångsbestämmelsen uppfyller kraven i artikel 3.

7.3.2 Olaglig systemstörning (artikel 4)

Bedömning: Svensk rätt uppfyller genom främst dataintrångsbestämmelsen direktivets krav på vilka handlingar som ska vara straffbelagda som olaglig systemstörning.

Skälen för bedömningen

Enligt *artikel 4* ska det vara straffbart att 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, när gärningen begås med uppsåt och orättmätigt, åtminstone i fall som inte är ringa.

Bestämmelsen överensstämmer helt med artikel 3 i rambeslutet. Den överensstämmer även i stort med artikel 5 om systemstörning i konventionen.

Vid genomförandet av rambeslutet i svensk rätt straffbelades som dataintrång enligt 4 kap. 9 c § brottsbalken bl.a. att blockera en uppgift som är avsedd för automatiserad behandling (se närmare avsnitt 5.3.2). Vidare utvidgades dataintrångsbestämmelsen till att omfatta även den som olovligen, genom någon annan liknande åtgärd än de som uttryckligen räknas upp i bestämmelsen, allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling. Genom ändringarna av dataintrångsbestämmelsen ansågs svensk rätt uppfylla den aktuella artikeln i rambeslutet (prop. 2006/07:66 s. 25–27 och 43–45).

I avsnitt 5.3.6 har vi gjort bedömningen att svensk rätt genom främst dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som systemstörning. I avsnittet konstateras vidare att vissa av de förfaranden som beskrivs som systemstörning i svensk rätt i vissa fall även kan tänkas motsvara andra brott, främst skadegörelse och sabotage, när handlandet samtidigt innebär att datorer eller program skadas. Eftersom direktivets artikel om olaglig systemstörning i allt väsentligt motsvarar konventionens artikel om systemstörning är analysen i avsnittet av relevans även för frågan om svensk rätt lever upp till direktivets krav i denna del. Vi hänvisar därför till denna analys.

Mot den angivna bakgrunden är vår bedömning att svensk rätt genom främst dataintrångsbestämmelsen uppfyller kraven i artikel 4.

7.3.3 Olaglig datastörning (artikel 5)

Bedömning: Svensk rätt uppfyller genom främst dataintrångsbestämmelsen direktivets krav på vilka handlingar som ska vara straffbelagda som olaglig datastörning.

Skälen för bedömningen

Enligt *artikel 5* ska det vara straffbart att radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, när gärningen begås med uppsåt och orättmätigt, åtminstone i fall som inte är ringa.

Bestämmelsen överensstämmer helt med artikel 4 i rambeslutet. Den överensstämmer även i stort med artikel 4 om datastörning i konventionen.

Som nämnts i föregående avsnitt straffbelades vid genomförandet av rambeslutet i svensk rätt som dataintrång bl.a. att blockera en uppgift som är avsedd för automatiserad behandling (se närmare avsnitt 5.3.2). Genom denna ändring av dataintrångsbestämmelsen ansågs svensk rätt uppfylla den aktuella artikeln i rambeslutet (prop. 2006/07:66 s. 27–28 och 42–43).

I avsnitt 5.3.5 har vi gjort bedömningen att svensk rätt genom främst dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som datastörning. I avsnittet konstateras vidare att de förfaranden som beskrivs som datastörning i vissa fall även kan tänkas motsvara andra brott i svensk rätt, främst skadegörelse och sabotage, och att grov skadegörelse, sabotage och grovt sabotage dessutom är straffbart som terroristbrott enligt lagen (2003:148) om straff för terroristbrott under de förutsättningar som anges i den lagen. Eftersom direktivets artikel om olaglig datastörning i allt väsentligt motsvarar konventionens artikel om datastörning är analysen i avsnittet av relevans även för frågan om svensk rätt lever upp till direktivets krav i denna del. Vi hänvisar därför till denna analys.

Mot den angivna bakgrunden är vår bedömning att svensk rätt genom främst dataintrångsbestämmelsen uppfyller kraven i artikel 5.

7.3.4 Olaglig avlyssning (artikel 6)

Bedömning: Svensk rätt uppfyller genom bestämmelsen om brytande av post- eller telehemlighet och dataintrångsbestämmelsen direktivets krav på vad som ska vara straffbelagt som olaglig avlyssning.

Skälen för bedömningen

Enligt *artikel 6* ska avlyssning med tekniska hjälpmedel av icke-offentliga överföringar av datorbehandlingsbara uppgifter till, från eller inom ett informationssystem, inklusive elektromagnetisk strålning från informationssystem som innehåller sådana uppgifter, straffbeläggas när gärningen begås med uppsåt och orättmätigt, åtminstone i fall som inte är ringa. Enligt beaktandesats 5a omfattar avlyssning, men är inte nödvändigtvis begränsat till, avlyssning och övervakning av kommunikationsinnehåll och framskaffande av uppgifter, antingen direkt genom åtkomst till och användning av informationssystem eller indirekt med tekniska hjälpmedel, genom användning av olika typer av elektroniska avlyssningsanordningar. Definitionen är huvudsakligen hämtad från konventionens förklarande rapport (p. 53, se avsnitt 5.3.4).

Bestämmelsen har inte någon motsvarighet i rambeslutet. Den överensstämmer emellertid i princip med artikel 3 om olaglig avlyssning i konventionen. Enligt konventionsartikeln får emellertid en stat, till skillnad från vad som gäller enligt direktivets bestämmelse, uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

I avsnitt 5.3.4 har vi gjort bedömningen att svensk rätt genom bestämmelsen om brytande av post- eller telehemlighet och dataintrångsbestämmelsen uppfyller konventionens krav på vad som ska vara straffbelagt som olaglig avlyssning. Vi har därvid gjort bedömningen att Sverige inte behöver uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem vid ett tillträde till konventionen. Eftersom direktivets artikel om olaglig avlyssning i allt väsentligt motsvarar konventionens artikel om olaglig avlyssning är analysen i avsnittet av relevans även för frågan om svensk rätt lever upp till direktivets krav i denna del. Vi hänvisar därför till denna analys.

Mot den angivna bakgrunden är vår bedömning att svensk rätt genom bestämmelsen om brytande av post- eller telehemlighet och dataintrångsbestämmelsen uppfyller kraven i artikel 6.

7.3.5 Verktyg som används för att begå brott (artikel 7)

Bedömning: Svensk rätt uppfyller genom bestämmelserna om förberedelse till brott direktivets krav på vilka befattningar med verktyg som ska vara straffbara.

Skälen för bedömningen

Enligt *artikel 7* ska det vara straffbart att tillverka, sälja, anskaffa i syfte att använda, importera, distribuera eller på annat sätt tillgängliggöra vissa uppräknade verktyg, om gärningen begås med uppsåt och orättmätigt, i syfte att begå något av de brott som avses i artiklarna 3–6, åtminstone i fall som inte är ringa.

De verktyg som räknas upp är

- ett datorprogram som utformats eller anpassats i första hand för att begå något av de brott som avses i artiklarna 3–6, samt
- ett lösenord, en åtkomstkod eller liknande uppgifter som gör det möjligt att få tillgång till ett informationssystem eller delar av ett sådant system.

Bestämmelsen har inte någon motsvarighet i rambeslutet, men överensstämmer i stort med artikel 6 om missbruk av apparatur i konventionen. Enligt artikel 6 i konventionen (punkt 1 b) ska det emellertid även vara straffbart att *inneha* sådant som räknas upp i artikeln. Något motsvarande krav på att straffbelägga innehav finns inte i direktivet.

Enligt beaktandesats 9 är verktyg i den mening som avses i direktivet exempelvis sabotageprogram, inklusive sådana som kan skapa s.k. botnät, som används för angrepp mot informationssystem. Även om ett verktyg är lämpat eller till och med särskilt lämpat för de brott som upptas i direktivet kan verktyget vara tillverkat för lagliga ändamål. Eftersom det finns ett behov av att undvika kriminalisering av fall där sådana verktyg tillverkas och saluförs för lagliga ändamål, t.ex. för test av informationsteknikprodukters funktionssäkerhet eller informationssystems säkerhet, måste, enligt beaktandesatstexten, utöver det allmänna kravet på uppsåt, också ett krav på direkt uppsåt uppfyllas, dvs. att verktygen är avsedda att användas för att begå något av de brott som upptas i direktivet. Motsvarande förklaring om krav på direkt uppsåt finns i

artikel 6.2 i konventionen (se även den förklarande rapporten p. 76 och 77).

I avsnitt 5.3.7 har vi gjort bedömningen att svensk rätt genom bestämmelserna om förberedelse till brott uppfyller konventionens krav på vad som ska vara straffbelagt som missbruk av apparatur. I avsnittet har även nämnts att olika former av tillgängliggörande av de olika hjälpmedel som avses i konventionsbestämmelsen i syfte att begå något av brotten i konventionen enligt svensk rätt även skulle kunna innefatta medverkan till brotten och att även medverkan till förberedelse är straffbart. Eftersom direktivets artikel om verktyg som används för att begå brott i allt väsentligt motsvarar konventionens artikel om missbruk av apparatur, är analysen i avsnittet av relevans även för frågan om svensk rätt lever upp till direktivets krav i denna del. Vi hänvisar därför till denna analys.

Mot den angivna bakgrunden är vår bedömning att svensk rätt genom bestämmelserna om förberedelse till brott uppfyller kraven i artikel 7 och att vissa av de förfaranden som beskrivs i artikeln i svensk rätt även skulle kunna utgöra medverkan till brott.

7.3.6 Anstiftan, medhjälp och försök (artikel 8)

Bedömning: Svensk rätt uppfyller direktivets krav på kriminalisering av dels anstiftan av och medhjälp till brotten i artiklarna 3–7, dels försök till brotten i artiklarna 4 och 5.

Skälen för bedömningen

I *artikel 8* finns krav på kriminalisering av osjälvständiga brottsformer.

Enligt *artikel 8.1* ska anstiftan av och medhjälp till brotten i artiklarna 3–7 vara straffbart.

I *artikel 8.2* föreskrivs att försök att begå brotten i artiklarna 4 och 5 ska vara straffbart.

En motsvarande bestämmelse finns i artikel 5 i rambeslutet. Enligt konventionens bestämmelse om kriminalisering av osjälvständiga brottsformer (artikel 11) krävs inte uttryckligen att anstiftan straffbeläggs.

Bestämmelserna om anstiftan och medhjälp i 23 kap. 4 § brottsbalken gäller vid alla brottsbalksbrott samt de brott i special-

straffrätten för vilka fängelse är föreskrivet eller för vilka särskild föreskrift finns att medverkan ska bestraffas (se även avsnitt 5.3.12). Anstiftan av och medhjälp till brytande av post- eller telehemlighet, dataintrång, skadegörelse, grov skadegörelse, sabotage, grovt sabotage och terroristbrott är alltså straffbart. Även anstiftan av och medhjälp till förberedelsebrott är straffbart.

I svensk rätt är således anstiftan av och medhjälp till samtliga de brott som vi i avsnitt 7.3.1–7.3.5 ansett motsvara de brott som upptas i artiklarna 3–7 straffbart.

Försök till brott är enligt 23 kap. 1 § brottsbalken straffbart i de fall det finns ett särskilt stadgande om det. Vi har i avsnitt 7.3.2 och 7.3.3 gjort bedömningen att svensk rätt uppfyller direktivets krav på kriminalisering av brotten i artiklarna 4 och 5 främst genom bestämmelsen om dataintrång, men samtidigt angett att straffansvar i vissa fall även skulle kunna aktualiseras enligt bestämmelserna om skadegörelse, sabotage och terroristbrott.

Försök till dataintrång är straffbart under förutsättning att intrånget inte skulle ha varit att anse som ringa om det hade fullbordats (4 kap. 10 § brottsbalken). Även försök till skadegörelse och grov skadegörelse (12 kap. 5 § brottsbalken), sabotage och grovt sabotage (13 kap. 12 § brottsbalken) och terroristbrott (4 § lagen [2003:148] om straff för terroristbrott) är straffbart.

Sammanfattningsvis uppfyller svensk rätt alltså direktivets krav på kriminalisering av dels anstiftan av och medhjälp till brotten i artiklarna 3–7, dels försök till brotten i artiklarna 4 och 5.

7.3.7 Påföljder (artikel 9)

Bedömning: Svensk rätt uppfyller i stort direktivets bestämmelser om påföljder. Det krävs dock lagstiftning för att uppfylla direktivets krav på att dels samtliga sådana straffbara befattningar med verktyg som avses i artikel 7 ska vara belagda med ett maximistraff på minst två års fängelse, dels brotten olaglig systemstörning och olaglig datastörning i de fall som avses i artikel 9.3 och 9.4 ska vara belagda med ett maximistraff på minst tre respektive fem års fängelse.

Skälen för bedömningen

Artikel 9 innehåller både generella och artikelspecifika bestämmelser om vilka påföljder som ska kunna dömas ut för brotten i direktivet.

Enligt *punkt 1* ska brotten i direktivet generellt ha påföljder som är effektiva, proportionerliga och avskräckande. Enligt beaktandesats 6 bör påföljderna inbegripa fängelsestraff eller ekonomiska påföljder.

Enligt *punkt 2* ska samtliga brott i direktivet, undantaget osjälvständiga brottsformer (dvs. de brott som avses i artikel 8) och ringa brott, ha en straffskala med ett maximistraff på minst två års fängelse.

För brotten *olaglig systemstörning* (artikel 4) och *olaglig datastörning* (artikel 5) krävs enligt *punkt 3* dessutom ett lägsta maximistraff på tre års fängelse när ett betydande antal informationssystem har påverkats genom användning av ett verktyg som har utformats eller anpassats primärt för detta syfte.

För brotten *olaglig systemstörning* och *olaglig datastörning* ställs vidare enligt *punkt 4* ett krav på ett lägsta maximistraff på fängelse i fem år under tre alternativa förutsättningar:

a) att brottet har begåtts inom ramen för en kriminell organisation enligt definitionen i rambeslut 2008/814/RIF, oberoende av den påföljdsnivå som anges där,

b) att brottet har orsakat allvarlig skada, eller

c) att brottet har begåtts mot ett kritiskt informationsinfrastruktursystem.

Enligt *punkt 5* ska det kunna anses som en försvårande omständighet i den nationella lagstiftningen när brotten *olaglig systemstörning* och *olaglig datastörning* begås genom missbruk av personuppgifter som rör en annan person än gärningsmannen, i syfte att vinna tredje mans förtroende, och därigenom medför skada för den som identiteten tillhör, om inte dessa omständigheter redan täcks av ett annat brott som är straffbart enligt nationell lagstiftning.

En motsvarande bestämmelse som den som finns i punkt 1 finns i artikel 13.1 i konventionen (se avsnitt 5.3.14) och i artikel 6.1 i rambeslutet. I konventionen finns ingen specifik bestämmelse om straffskalornas utformning. I rambeslutet finns en bestämmelse som till viss del motsvarar punkt 2. I artikel 6.2 i rambeslutet föreskrivs nämligen att brotten olaglig systemstörning (artikel 3 i

rambeslutet) och olaglig datastörning (artikel 4 i rambeslutet) ska vara belagda med straffrättsliga påföljder som innebär ett maximistraff på minst ett till tre års fängelse. I rambeslutet finns även bestämmelser som till viss del motsvarar punkt 4 (artikel 7 i rambeslutet). Enligt rambeslutet räcker det emellertid att fängelse i åtminstone två år finns i straffskalan. Punkt 4 kräver, som framgått, att fängelse i fem år ska finnas i straffskalan.

Vi har i tidigare avsnitt gjort bedömningen att svensk rätt uppfyller direktivets krav på kriminalisering av de gärningar som avses i artiklarna 3–6 genom främst bestämmelserna om brytande av post- eller telehemlighet och dataintrång, men att ansvar för dessa gärningar i vissa fall även kan komma i fråga enligt bestämmelserna om skadegörelse och sabotage.

Straffskalan för såväl brytande av post- eller telehemlighet som dataintrång är böter eller fängelse i högst två år. För skadegörelse och grov skadegörelse är straffskalorna böter eller fängelse i högst ett år respektive fängelse i högst fyra år. Straffskalorna för sabotage och grovt sabotage är fängelse i högst fyra år respektive fängelse på viss tid, lägst två och högst tio år, eller på livstid. Samtliga brott, utom skadegörelse av normalgraden har alltså ett maximistraff om minst två års fängelse. I fråga om gradindelade brott är det dock enligt vår mening tillräckligt att den grövsta formen – i detta fall grov skadegörelse – motsvarar vad som krävs enligt direktivet (jfr motsvarande bedömning av regeringen vid genomförandet av rambeslutet, prop. 2006/07:66 s. 29). Följaktligen uppfyller svensk rätt direktivets krav enligt punkterna 1 och 2 såvitt avser brotten i artiklarna 3–6.

När det gäller direktivets krav på kriminalisering av sådan befattning med verktyg som avses i artikel 7 har vi i tidigare avsnitt gjort bedömningen att svensk rätt uppfyller kravet genom bestämmelserna om förberedelse till brott men samtidigt att vissa av de förfaranden som beskrivs i artikeln i svensk rätt även skulle kunna utgöra medverkan till brott.

Förberedelse till brytande av post- eller telehemlighet är genom visst angivet förfarande straffbelagt i en särskild bestämmelse i 4 kap. 9 b § brottsbalken. Straffskalan enligt denna bestämmelse är böter eller fängelse i högst två år och alltså förenlig med punkterna 1 och 2.

Förberedelse till dataintrång är straffbart, om det fullbordade brottet inte skulle ha varit att anse som ringa. Även förberedelse till grov skadegörelse, sabotage och grovt sabotage är straffbart.

Straffet för förberedelse ska, enligt 23 kap. 2 § tredje stycket brottsbalken, bestämmas under den högsta och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre straff än fängelse i två år får bestämmas endast om fängelse i åtta år eller däröver kan följa på det fullbordade brottet.

Fängelse i två år finns alltså i straffskalan för förberedelse till grov skadegörelse, sabotage och grovt sabotage. Straffskalorna för dessa brott är alltså förenliga med punkterna 1 och 2. För förberedelse till dataintrång kan dock aldrig, mot bakgrund av att straffskalan för dataintrång är böter eller fängelse i högst två år och straffet för förberedelse ska bestämmas *under* den högsta gränsen som gäller för fullbordat brott, dömas till två års fängelse. I teorin är alltså det högsta straff som kan utdömas för förberedelse till dataintrång fängelse ett år och 364 dagar. Straffskalan för förberedelse till dataintrång är därför möjligtvis förenlig med punkt 1 men inte med det specifika kravet på ett maximistraff på minst två års fängelse i punkt 2. Det krävs därför lagändring för att uppfylla direktivets krav i denna del. I sammanhanget bör dock även framhållas att för det fall en sådan gärning som avses i artikel 7 i svensk rätt är att anse som medverkan till dataintrång uppfyller svensk rätt kravet på påföljd av visst slag.

Osjälvständiga brottsformer omfattas, som framgått, inte av kravet på visst maximistraff enligt punkt 2. De ska dock, enligt punkt 1, vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder. För anstiftan av och medhjälp till brytande av post- eller telehemlighet, dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage kan dömas till fängelse. Detsamma gäller försök att begå dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage. Mot den bakgrunden gör vi bedömningen att svensk rätt uppfyller kravet enligt punkt 1 såvitt avser brotten i artikel 8.

Punkterna 3, 4 och 5 gäller, som framgått, enbart brotten olaglig systemstörning och olaglig datastörning. Enligt punkt 3 ska dessa brott ha ett maximistraff på minst tre års fängelse när ett stort antal informationssystem har påverkats genom användning av ett verktyg som har utformats primärt för detta syfte och enligt punkt 4 ställs krav på ett lägsta maximistraff på fängelse i fem år för dessa brott under vissa förutsättningar.

Vi har i avsnitt 7.3.2 och 7.3.3 gjort bedömningen att svensk rätt genom främst dataintrångsbestämmelsen uppfyller direktivets krav på vilka handlingar som ska vara straffbelagda som olaglig system-

störning och olaglig datastörning. Straffskalan för dataintrång är, som tidigare nämnts, böter eller fängelse i högst två år. Dataintrångsbestämmelsen med sin nuvarande straffskala är således inte tillräcklig för att motsvara direktivets krav på ett maximistraff på minst tre respektive fem års fängelse enligt punkt 3 respektive 4.

Som redogjorts för i avsnitt 7.3.2 och 7.3.3 kan emellertid de gärningar som i direktivet avses med olaglig systemstörning och olaglig datastörning i svensk rätt i vissa fall även tänkas motsvara andra brott, främst skadegörelse och sabotage. Grov skadegörelse, sabotage och grovt sabotage är dessutom straffbart som terroristbrott enligt lagen (2003:148) om straff för terroristbrott under de förutsättningar som anges i den lagen.

För skadegörelse och grov skadegörelse är, som nämnts, straffskalorna böter eller fängelse i högst ett år respektive fängelse i högst fyra år. Straffskalorna för sabotage och grovt sabotage är fängelse i högst fyra år respektive fängelse på viss tid, lägst två och högst tio år, eller på livstid. För terroristbrott är straffet fängelse på viss tid, lägst fyra och högst 18 år, eller på livstid. Är brottet mindre grovt, är straffet fängelse, lägst två år och högst sex år.

För det fall de gärningar som avses i punkt 3 träffas av straffansvaret för grov skadegörelse, sabotage eller grovt sabotage och de gärningar som avses i punkt 4 på motsvarande sätt träffas av straffansvaret för grovt sabotage, alternativt om någon av gärningarna skulle vara att anse som terroristbrott, uppfyller svensk rätt således kraven på vilka påföljder som ska kunna dömas ut enligt punkterna.

Skadegörelsebestämmelserna avser i huvudsak angrepp på egendom som medför att egendomen förstörs eller skadas. Normalt förutsätts att saken verkligen undergår en förändring och att skadan inte är av endast tillfällig natur (jfr Berggren m.fl., *Brottsbalken En kommentar kap. 1–12*, s. 12:3). I stor utsträckning gäller det även sabotagebestämmelserna. Sabotagebestämmelserna är emellertid tillämpliga även då användningen av viss närmare angiven egendom allvarligt störs eller hindras utan att denna förstörts eller skadats.

Straffbestämmelserna kan således tillämpas i vissa fall när handlandet *samtidigt* innebär att datorer eller program skadas.

Med olaglig systemstörning (artikel 4) avses enligt direktivet 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. Förfarandet behöver inte innebära att datorer eller program skadas. Vid exempelvis olika former

av överbelastningsattacker eller tillgänglighetsattacker som riktar sig mot själva systemet och dess funktion, och vars syfte t.ex. kan vara att göra en webbplats otillgänglig, är skadan oftast av tillfällig karaktär. Bestämmelserna om skadegörelse och sabotage är då inte omedelbart tillämpliga.

På samma sätt förhåller det sig när det gäller den gärning som i direktivet avses med olaglig datastörning (artikel 5). Gärningen beskrivs som att uppsåtligen och orättmätigt radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem. Inte heller detta förfarande behöver innebära att datorer eller program, eller ens befintliga uppgifter i systemet, skadas. Överbelastnings- eller tillgänglighetsattacker kan innebära just att flödet av datorbehandlingsbara uppgifter i ett informationssystem hindras och att det blir omöjligt att komma åt uppgifterna, utan att skadan är av annat än tillfällig karaktär.

När det gäller sabotagebrottet krävs för straffansvar vidare att *för samhället viktig egendom* förstörs eller skadas eller att användningen av sådan egendom allvarligt störs eller hindras.

Den brottsliga gärningen kan uttryckas så att någon ska skada, förstöra eller allvarligt hindra användningen av ett *sabotageobjekt* (se Ulväng m.fl., *Brotten mot allmänheten och staten*, 2012, s, 26–27).

Som sabotageobjekt upptas, enligt 13 kap. 4 § brottsbalken:

1. egendom som har avsevärd betydelse för
   a. rikets försvar, folkförsörjning, rättsskipning eller förvaltning, eller
   b. upprätthållande av allmän ordning och säkerhet i riket,
2. den allmänna samfärdseln,
3. telegraf, telefon, radio, eller dylikt hjälpmedel, och
4. anläggning för allmänhetens förseende med vatten, ljus, värme eller kraft.

Gärningar som riktar sig mot objekt enligt *1* ska innebära att egendomen *skadas* eller *förstörs* eller att dess *användning allvarligt störs* eller *hindras*. Gärningar som riktar sig mot objekt enligt *2–4* ska innebära att objektets *användning allvarligt störs* eller *hindras*.

Som exempel på sådana sabotageobjekt som faller under 1 har nämnts befästningsanläggningar, kaserner, förråd av större betydelse, för folkförsörjningen viktiga fabriker och gruvor, statliga och

kommunala myndigheters lokaler samt polis- och brandstationer (Berggren m.fl., *Brottsbalken En kommentar kap. 13–24*, s. 13:17).

Som framgått ska enligt punkt 3 brotten olaglig systemstörning och olaglig datastörning ha ett lägsta maximistraff på tre års fängelse när ett betydande antal informationssystem har påverkats genom användning av ett verktyg som har utformats primärt för detta syfte. Det förfarande som åsyftas är bl.a. användning av s.k. botnät, då ett stort antal datorer kan tas över och fjärrstyras till följd av att de har infekterats av sabotageprogram genom riktade it-angrepp (se beaktandesats 3). I ett senare skede kan de smittade datorerna, som utgör botnätet, utan användarnas vetskap aktiveras för storskaliga it-angrepp.

Även om en tillgänglighetsattack eller en attack av något annat slag har fått till följd att ett stort antal informationssystem har påverkats, och exempelvis har fått till följd att ett betydande antal webbplatser blivit otillgängliga eller att ett stort antal datorer tagits över, är det långt ifrån klart att sabotagebestämmelsen blir tillämplig. Förutom att skadan kan vara av tillfällig karaktär är det inte säkert att de informationssystem som påverkats kan anses utgöra sådan för samhället viktig egendom att de kan anses utgöra sabotageobjekt.

Enligt punkt 4 ska vidare, som framgått, brotten olaglig systemstörning och olaglig datastörning ha ett lägsta maximistraff på fem års fängelse när de a) begås inom ramen för en kriminell organisation, b) förorsakar allvarlig skada, eller c) begås mot ett kritiskt infrastruktursystem. De enskilda medlemsstaterna får själva fastställa vad som utgör allvarlig skada enligt sin nationella lagstiftning och praxis. Enligt beaktandesats 3 kan som sådan emellertid bl.a. betraktas störning av systemtjänster av stort allmänintresse, orsakande av stora ekonomiska kostnader eller förlust av personuppgifter eller känslig information. Med kritisk infrastruktur avses enligt beaktandesats 2a anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga t.ex. för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, försörjningstrygghet och ekonomisk eller social välfärd såsom kraftverk, transportnät eller nätverk av myndigheter och där driftstörning eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner.

Gärningar under c kan i många fall omfattas av sabotagebestämmelsen. När det gäller gärningar under b däremot kan mycket väl

tänkas situationer där olika former av angrepp och attacker mot informationssystem orsakar betydande ekonomiska skador på grund av avbrott i informationssystemens drift och kommunikation, men där sabotagebestämmelsen inte skulle bli tillämplig, antingen för att skadan är av tillfällig karaktär eller för att inte sådan för samhället viktig egendom som avses i sabotagebestämmelsen skadats. Även om skadegörelsebestämmelsen skulle vara tillämplig är straffskalan för grov skadegörelse otillräcklig, eftersom den enbart sträcker sig till fyra års fängelse. Inte heller är det självklart att sabotagebestämmelsen skulle bli tillämplig för gärningar under a.

Vår bedömning är att det krävs lagstiftningsåtgärder för att uppfylla direktivets krav på påföljder enligt såväl punkt 3 som 4.

Punkt 5 ställer, som framgått, krav på att det ska kunna anses som en försvårande omständighet när brotten olaglig systemstörning och olaglig datastörning begås genom missbruk av personuppgifter. Uppgifterna ska avse annan person än gärningsmannen, syftet ska vara att vinna tredje mans förtroende och handlandet ska medföra skada för den som identiteten tillhör. Om dessa omständigheter redan täcks av ett annat brott som är straffbart i nationell lagstiftning, behöver de inte anses som försvårande inom ramen för brotten olaglig systemstörning och olaglig datastörning.

Införandet av effektiva åtgärder mot identitetsstöld och andra identitetsrelaterade brott utgör enligt beaktandesats 7a en viktig del i en samlad ansats mot it-brottslighet. De förfaranden som punkt 5 främst torde avse är sådana där gärningsmannen bereder sig tillgång till en legitim användares IP-adress och därigenom får tillgång till denne persons användarkonton och därefter sänder ”skräddarsydd” bedräglig e-post till specifikt utvalda mål eller grupper inom en organisation. Genom den stora massan av allmänt tillgänglig personlig information om ledande befattningshavare och offentliga personer som i dag finns på olika sociala nätverk har denna typ av brott blivit allt enklare att begå. Med hjälp av sådan personlig information kan gärningsmannen nämligen skapa ett trovärdigt e-postmeddelande som kan innehålla trojaner eller andra typer av sabotageprogram. Eftersom den som mottar e-posten får uppfattningen att denna kommer från en pålitlig källa öppnar han eller hon den och sabotageprogrammen installeras därmed på värddatorn. Sabotageprogrammet kan sedan exempelvis ge gärningsmannen fri tillgång till den angripna organisationens eller personens server.

I svensk rätt motsvaras, som nämnts, brotten olaglig systemstörning och olaglig datastörning främst av brottet dataintrång.

Någon försvårande omständighet hänförlig till identitetsstöld anges inte i dataintrångsbestämmelsen. Enligt 29 kap. 2 § 2, 3 och 6 brottsbalken ska emellertid som försvårande omständighet vid bedömningen av straffvärdet, vid sidan av vad som gäller för varje särskild brottstyp, särskilt beaktas om den tilltalade visat stor hänsynslöshet (punkt 2), utnyttjat någon annans skyddslösa ställning eller svårighet att värja sig (punkt 3) eller om brottet exempelvis föregåtts av särskild planering (punkt 6).

Punkterna 2 och 3 skulle kunna vara tillämpliga i vissa situationer. Punkt 6 kan, som framgått, tillämpas bl.a. om brottet föregåtts av särskild planering. Så kan anses vara fallet om någon utnyttjat annans personuppgifter på det sätt som avses i artikel 9.5. Missbruk av personuppgifter kan även ske på ett sådant sätt att de svenska bestämmelserna om exempelvis bedrägeri, urkundsförfalskning och förtal blir tillämpliga.

Sammanfattningsvis gör vi bedömningen att det inte omedelbart krävs några lagstiftningsåtgärder för att leva upp till kraven i punkt 5.

7.3.8 Ansvar och påföljder för juridiska personer (artiklarna 11 och 12)

Bedömning: Svensk rätt får genom bestämmelserna om företagsbot och förverkande anses uppfylla de krav som direktivet ställer i fråga om ansvar och påföljder för juridiska personer.

Skälen för bedömningen

I *artiklarna 11* och *12* finns bestämmelser om ansvar och påföljder för juridiska personer. Med juridisk person avses enligt artikel 1 c, som nämnts i avsnitt 7.2, enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer. Som tidigare nämnts förekommer definitionen även i rambeslutet.

Bestämmelserna om ansvar och påföljder för juridiska personer innebär att påföljder i form av bötesstraff eller administrativa avgifter under vissa förutsättningar ska kunna åläggas sådana per-

soner när brott har begåtts till deras förmån. Något krav på att införa straffrättsligt ansvar finns alltså inte.

Motsvarande bestämmelser finns i rambeslutet (artiklarna 8–9) och i konventionen (artiklarna 12 och 13.2).

Vid genomförandet av rambeslutet i svensk rätt gjorde regeringen bedömningen att de svenska reglerna om företagsbot fick anses motsvara de krav som ställs i rambeslutets artikel 8 och 9 (prop. 2006/07:66 s. 31). Vi har i avsnitt 5.3.13 gjort motsvarande bedömning när det gäller konventionens krav på ansvar och påföljder för juridiska personer. I avsnittet hänvisas även till möjligheten i svensk rätt att förverka värdet av ekonomiska fördelar som uppkommit för näringsidkare vid brott i näringsverksamhet. I avsnittet finns en redogörelse över de svenska bestämmelserna om företagsbot och förverkande.

Vi gör bedömningen att de svenska reglerna om företagsbot och förverkande även i fråga om direktivet får anses motsvara de krav som ställs i artiklarna 11 och 12 om ansvar och påföljder för juridiska personer.

7.4 Domsrätt (artikel 13)

Bedömning: Direktivets krav på behörighet (domsrätt) motsvarar svenska bestämmelser på området. Sverige bör i den ordning som föreskrivs i direktivet lämna underrättelse om att svenska regler om domsrätt innebär en mer vidsträckt behörighet över brott som begåtts utomlands än direktivet kräver, t.ex. när gärningsmannen har sin hemvist i Sverige.

Skälen för bedömningen

I *artikel 13* finns bestämmelser om behörighet (domsrätt).

Enligt *punkt 1 a* ska en medlemsstat ha domsrätt i fråga om brott enligt direktivet som har ägt rum helt eller delvis på medlemsstatens territorium. Enligt *punkt 2* ska behörigheten innefatta situationer där a) gärningsmannen är fysiskt närvarande på medlemsstatens territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på denna medlemsstats territorium eller inte, eller b) brottet riktar sig mot ett informationssystem på

medlemsstatens territorium oavsett om gärningsmannen är fysiskt närvarande på detta territorium när brottet begås eller inte.

Enligt svenska regler om domsrätt döms efter svensk lag och vid svensk domstol för brott som begåtts här i riket (2 kap. 1 § brottsbalken). Detsamma gäller om det är ovisst var ett brott har förövats men det finns skäl att anta att det har begåtts inom riket. Ett brott anses begånget där den brottsliga handlingen företogs men också där brottet fullbordades, eller, vid försök, där brottet skulle ha fullbordats (2 kap. 4 § brottsbalken). Så snart någon del av handlingen har ägt rum här i riket är alltså handlingen i sin helhet att anse som begången i Sverige.

Motsvarande bestämmelser om domsrätt finns i rambeslutet (artikel 10.1 a och 10.2). Vid genomförandet av rambeslutet i svensk rätt gjorde regeringen bedömningen att de svenska regler om domsrätt som nyss redogjorts för, ger svenska domstolar behörighet att döma över brott i de fall som nu avses, och att bestämmelserna därför uppfyllde rambeslutet i dessa avseenden (prop. 2006/07:66 s. 32). Vi gör motsvarande bedömning såvitt avser direktivets krav på domsrätt i de fall som avses i punkt 1 a och 2. Någon lagändring krävs alltså inte.

Enligt *punkt 1 b* ska varje medlemsstat ha domsrätt beträffande brott enligt direktivet som har begåtts av en av medlemsstatens medborgare, åtminstone i sådana fall där gärningen utgör ett brott på den plats där den begicks.

En motsvarande bestämmelse om domsrätt finns även i rambeslutet (artikel 10.1 b). Enligt den bestämmelsen får emellertid inte, till skillnad från direktivsbestämmelsen, krav uppställas på dubbel straffbarhet för domsrätt.

Enligt svensk rätt döms för brott som begåtts utom riket efter svensk lag vid svensk domstol bl.a. om brottet har begåtts av en svensk medborgare (2 kap. 2 § 1 brottsbalken). För att svensk domsrätt ska föreligga för sådana brott krävs dock normalt att gärningen är straffbar där den begicks (krav på dubbel straffbarhet). Vidare får inte dömas till påföljd som är att anse som strängare än det svåraste straff som är föreskrivet för brottet enligt lagen på gärningsorten.

Svensk rätt uppfyller således även åtagandet i punkt 1 b, eftersom krav på dubbel straffbarhet får uppställas enligt punkten. Någon lagändring krävs alltså inte (jfr motsvarande bedömning vid genomförandet av rambeslutet, prop. 2006/07:66 s. 32).

Enligt *punkt 3* ska en medlemsstat underrätta kommissionen om den beslutar att fastställa ytterligare domsrätt över ett brott enligt

artikel 3–8 som har begåtts utanför dess territorium, t.ex. när a) gärningsmannen har sin hemvist på denna medlemsstats territorium, eller b) när gärningen har begåtts till förmån för en juridisk person som är etablerad inom denna medlemsstats territorium. Rambeslutet innehåller inte någon motsvarande bestämmelse.

Några krav på medlemsstaternas lagstiftning uppställs alltså inte i punkt 3. Eftersom svenska regler om domsrätt är vidsträckta och det generellt finns goda möjligheter att ingripa även mot brott som har begåtts utomlands, krävs emellertid att Sverige underrättar kommissionen om i vilka fall svensk domsrätt föreligger. Enligt 2 kap. 2 § brottsbalken döms exempelvis efter svensk lag och vid svensk domstol om brottet begåtts 1) av utlänning med hemvist i Sverige, 2) av utlänning utan hemvist i Sverige, som efter brottet blivit svensk medborgare eller tagit hemvist här i riket eller som är dansk, finsk, isländsk, eller norsk medborgare och finns här, eller 3) av annan utlänning som finns här i riket och på brottet enligt svensk lag kan följa fängelse i mer än sex månader. För att svensk domsrätt ska föreligga för sådana brott ställs dock normalt, liksom när det gäller brott begångna utomlands av svenska medborgare, krav på dubbel straffbarhet. Vidare får inte dömas till påföljd som är att anse som strängare än det svåraste straff som är föreskrivet för brottet enligt lagen på gärningsorten.

7.5 Informationsutbyte (artikel 14)

Bedömning: Bestämmelserna om informationsutbyte kräver inte lagstiftningsåtgärder. Sverige bör lämna underrättelse om att Rikspolisstyrelsen ska vara kontaktpunkt för utbytet av uppgifter.

Skälen för bedömningen

Enligt *artikel 14* ska medlemsstaterna för utbyte av uppgifter om de brott som avses i direktivet se till att ha en operativ nationell kontaktpunkt och använda det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan.

Det nät som åsyftas är – vilket framgår av beaktandesats 11 – det som omnämns i rådets rekommendation av den 25 juni 2001 om kontaktpunkter som upprätthåller ett öppethållande dygnet runt

för bekämpning av högteknologisk brottslighet (EGT C 187, 3.7.2001, s. 5). Detta nätverk skapades i G8, som utgörs av åtta ledande industriländer (prop. 2006/07:66 s. 33).

Enligt artikeln ska medlemsstaterna också se till att ha förfaranden som gör att de vid brådskande förfrågningar inom högst åtta timmar efter mottagandet kan ange åtminstone huruvida framställningen om bistånd kommer att besvaras samt formen och den beräknade tidpunkten för svaret.

Av artikeln följer vidare att varje medlemsstat ska underrätta kommissionen om sin kontaktpunkt.

Slutligen följer av artikeln att medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att lämpliga rapporteringskanaler är tillgängliga för att underlätta att de brott som avses i artiklarna 3–6 rapporteras till behöriga nationella myndigheter utan dröjsmål.

En motsvarande artikel om utbyte av uppgifter och utseende av kontaktpunkt finns i rambeslutet (artikel 11) och i konventionen (artikel 35). Enligt rambeslutets bestämmelse finns emellertid inte någon skyldighet att besvara en brådskande begäran om bistånd inom åtta timmar.

Vid genomförandet av rambeslutet i svensk rätt utsågs Rikspolisstyrelsen till Sveriges kontaktpunkt (prop. 2006/07:66 s. 34). Sverige har nämligen deltagit i G8-nätverket sedan 1999. Någon reglering för att uppfylla åtagandet om utbyte av uppgifter i rambeslutet ansågs mot den bakgrunden inte behövlig.

Vi gör motsvarande bedömning när det gäller åtagandet enligt direktivets artikel 14. När det gäller skyldigheten att besvara en brådskande begäran inom åtta timmar är den inte, mot bakgrund av att beskedet endast ska ange huruvida, i vilken form och när en begäran om hjälp kommer att besvaras, att förstå så att ett fullständigt svar i sak ska kunna lämnas inom fristen. Sverige bör således lämna underrättelse om att Rikspolisstyrelsen ska vara kontaktpunkt för utbytet av uppgifter. I avsnitt 5.6.14 har vi gjort samma bedömning när det gäller konventionens krav på nätverk. Som påpekats i det avsnittet kan det finnas skäl att, mot bakgrund av konventionsåtagandet, se över organisationen inom Rikspolisstyrelsen så att den enhet som i praktiken ska fungera som kontaktpunkt förfogar över de resurser som krävs för att fullgöra denna uppgift. Motsvarande gäller vid genomförandet av direktivet.

Vi gör bedömningen att Sverige även uppfyller det generella kravet på lämpliga kanaler för rapportering av brott.

7.6 Övervakning och statistik (artikel 15)

Bedömning: Bestämmelserna om övervakning och statistik kräver inte lagstiftningsåtgärder.

Skälen för bedömningen

Enligt *artikel 15* ska medlemsstaterna se till att det finns ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om brott som avses i direktivet, undantaget osjälvständiga brottsformer. De statistiska uppgifterna ska åtminstone omfatta befintliga uppgifter om *antalet brott* som registrerats av medlemsstaterna och *antalet personer* som åtalats och dömts för sådana brott. Medlemsstaterna ska översända de uppgifter som samlats in till kommissionen. Det åligger därefter kommissionen att se till att en samlad översikt över dessa statistiska rapporter offentliggörs och översänds till behöriga specialiserade unionsorgan och byråer.

Någon mot artikel 15 svarande artikel finns inte i rambeslutet eller konventionen.

I Sverige ansvarar Brottsförebyggande rådet (Brå) för den officiella rättsstatistiken. Brå sammanställer, publicerar och utvecklar Sveriges officiella kriminalstatistik. Statistikskyldigheten omfattar bl.a. brott och för brott lagförda personer (1 § andra stycket lagen [2001:99] om den officiella statistiken jfr med 2 § första stycket förordningen [2001:100] om den officiella statistiken jämte bilaga).

I den officiella rättsstatistiken ingår ärenden som handläggs av polis, tull, åklagare, domstol och kriminalvård. Statistiken bygger på de uppgifter som myndigheterna registrerar i sina administrativa system, i samband med utredningen av en misstänkt brottslig händelse, lagföring av en person som befunnits skyldig till brott och verkställande av en utdömd påföljd.

Brå:s uppdrag och arbete när det gäller den officiella rättsstatistiken innebär att Sverige uppfyller direktivets krav på system för registrering, insamling och tillhandahållande av statistiska uppgifter. Några lagstiftningsåtgärder krävs alltså inte mot bakgrund av artikel 15.

8 Genomförandet av konventionen och tilläggsprotokollet i svensk rätt

8.1 Inledning

I avsnitt 5 och 6 har analyserats vilket behov av lagändringar som konventionen respektive tilläggsprotokollet föranleder.

Vi har kommit fram till att svensk rätt redan uppfyller såväl konventionens som tilläggsprotokollets krav på *straffrättsliga* bestämmelser, under förutsättning att dels regeringens förslag till ett nytt urkundsbegrepp i 14 kap. 1 § brottsbalken antas av riksdagen (se prop. 2012/13:74 *Förfalsknings- och sanningsbrotten*), dels Sverige utnyttjar möjligheten att kräva sådant ytterligare rekvisit för straffansvar som avses i tilläggsprotokollets artikel 6.2 a.

Vad avser konventionens *processrättsliga* bestämmelser, till vilka tilläggsprotokollet hänvisar, har vi gjort bedömningen att lagstiftningsåtgärder krävs för att svensk rätt ska leva upp till konventionens krav såvitt avser skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och skyndsamt säkrande och partiellt röjande av trafikuppgifter (artikel 16 respektive 17). Vi bedömer också att det finns skäl att överväga att införa en sådan möjlighet till föreläggande att lämna information inom ramen för en husrannsakan som avses i artikel 19.4, även om svensk rätt formellt sett redan kan anses uppfylla de krav som ställs i artikeln genom reglerna om vittnesförhör inför rätta under en förundersökning. I övrigt anser vi att svensk rätt redan uppfyller de krav som ställs med hänsyn till de möjligheter till förbehåll som finns i artiklarna 20 och 21.

Vi har vidare gjort bedömningen att svensk rätt är förenlig med konventionens och tilläggsprotokollets bestämmelser om *domsrätt*.

När det gäller konventionens bestämmelser om *internationellt samarbete*, till vilka tilläggsprotokollet på samma sätt som när det gäller de processrättsliga bestämmelserna hänvisar, har vi kommit fram till att lagstiftningsåtgärder krävs för att svensk rätt ska leva upp till konventionens krav på rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och skyndsamt röjande av vissa trafikuppgifter (artikel 29 respektive 30, dvs. motsvarigheterna till artikel 16 och 17 på området för rättslig hjälp). I övrigt bedömer vi att svensk rätt redan uppfyller de krav som ställs.

Konventionens och tilläggsprotokollets *slutbestämmelser* föranleder enligt vår mening inte några lagändringar.

I vårt uppdrag ligger att ta ställning till i vilken utsträckning Sverige bör utnyttja möjligheten att göra förbehåll och att avge förklaring att ytterligare rekvisit uppställs. Vi ska vidare lämna förslag till de författningsändringar eller andra förändringar som krävs för att tillåta ett tillträde till konventionen och tilläggsprotokollet. I det följande ger vi förslag till hur konventionen och tilläggsprotokollet ska genomföras i svensk rätt.

8.2 Anpassningen av den straffrättsliga regleringen

8.2.1 Utgångspunkter

När det gäller konventionens straffrättsliga artiklar är det endast artikeln om datorrelaterad förfalskning (artikel 7) som kräver lagstiftningsåtgärder för att möjliggöra ett svenskt tillträde till konventionen. Samtidigt finns en möjlighet att kräva ytterligare rekvisit i form av krav på bedrägligt uppsåt för att straffansvar enligt artikeln ska gälla (jfr avsnitt 5.3.8). Enligt vår mening skulle i sådana fall förfarandet sannolikt vara att bedöma som förberedelse eller försök till bedrägeri. Som vi har redovisat i avsnitt 5.3.8 har regeringen lämnat förslag till ett nytt urkundsbegrepp i 14 kap. 1 § brottsbalken (se prop. 2012/13:74 *Förfalsknings- och sanningsbrotten*). Om förslagen i propositionen antas av riksdagen innebär det att svensk rätt genom bestämmelsen om urkundsförfalskning kommer att uppfylla konventionskravet i denna del fullt ut. Mot den bakgrunden avstår vi från att lämna något eget förslag i denna del.

När det gäller tilläggsprotokollets straffrättsliga artiklar krävs inte några lagstiftningsåtgärder för att Sverige ska kunna tillträda

protokollet, om möjligheten att kräva ytterligare rekvisit för straffansvar för sådant förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten som avses i artikel 6 används. Frågan om Sverige ska utnyttja denna möjlighet behandlas i avsnitt 8.2.2.

8.2.2 Bör möjligheten att kräva ytterligare rekvisit för straffansvar när det gäller förnekande, grovt förringande, gillande eller rättfärdigande av folkmord eller brott mot mänskligheten utnyttjas?

Förslag: Sverige ska, i enlighet med artikel 6.2 a och 12.3 i tilläggsprotokollet, förklara att krav uppställs på att förnekandet eller det grova förringandet 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.

Skälen för förslaget

I tilläggsprotokollets artikel 6.1 uppställs krav på kriminalisering av gärningar som innebär att någon uppsåtligen och orättmätigt med hjälp av ett datorsystem sprider eller på annat sätt för allmänheten tillgängliggör material som förnekar, grovt förringar, gillar eller rättfärdigar gärningar som enligt folkrätten eller vissa internationella domstolar utgör folkmord eller brott mot mänskligheten. Av artikel 6.2 a framgår att en fördragsslutande stat får uppställa krav på att förnekandet eller det grova förringande som avses i artikel 6.1 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.

I avsnitt 6.2.5 har vi gjort bedömningen att svensk rätt, genom främst bestämmelserna om hets mot folkgrupp och uppvigling, uppfyller artikelns krav på vad som ska vara straffbelagt, om krav uppställs på att förnekandet eller det grova förringandet görs med sådant uppsåt som anges i artikel 6.2 a. Någon anledning att inom ramen för en ratificering av tilläggsprotokollet föreslå ändringar i

de svenska straffbestämmelserna i syfte att kriminalisera samtliga gärningar som omfattas av artikel 6.1 ser vi inte, speciellt som sådana ändringar skulle kunna innebära en ytterligare begränsning av yttrandefriheten. Vi föreslår därför att Sverige utnyttjar den möjlighet som, enligt artikel 6.2 a och 12.3, finns att kräva ytterligare rekvisit för straffansvar. Sverige bör således förklara att krav uppställs på att förnekandet eller det grova förringandet 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.

8.3 Anpassningen av den processrättsliga regleringen

8.3.1 Utgångspunkter

Vi har i avsnitt 5.4 gjort bedömningen att svensk rätt till stor del redan uppfyller de krav som konventionen ställer, men att lagstiftningsåtgärder krävs såvitt avser skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och skyndsamt säkrande och partiellt röjande av trafikuppgifter (artikel 16 respektive 17) och att det finns skäl att överväga att införa en sådan möjlighet till föreläggande att lämna information inom ramen för en husrannsakan som avses i artikel 19.4. Vi anser också att förbehåll i vissa avseenden krävs för att svensk rätt ska uppfylla de krav som ställs i konventionens artiklar om insamling i realtid av trafikuppgifter (artikel 20) och avlyssning av innehållsuppgifter (artikel 21).

I avsnitt 6.3 har vi gjort bedömningen att det inte krävs några ytterligare lagändringar för att tillgodose de krav som följer av tilläggsprotokollet i fråga om processrättsliga regler än de som följer av konventionens processrättsliga bestämmelser.

I våra direktiv framhålls att i den mån vår analys föranleder förslag om nya straffprocessuella tvångsmedel eller ändringar i befintliga tvångsmedel, ska förslagen utformas på ett sådant sätt att tvångsmedelsanvändningen är proportionerlig i förhållande till det intrång i enskildas integritet som befogenheten innebär. Det framhålls vidare att det är angeläget att åstadkomma en så klar och överblickbar tvångsmedelsreglering som möjligt och att, vid utarbet-

ande av förslag till nya bestämmelser, hänsyn ska tas till den grundläggande systematiken i regleringen.

I följande avsnitt redovisas våra förslag till lagstiftning för att tillgodose konventionens krav på skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter (avsnitt 8.3.2) och möjlighet att få till stånd ett säkrande även om flera tjänsteleverantörer har deltagit vid överföringen av uppgifterna (avsnitt 8.3.3), liksom övervägan-den i frågan om en möjlighet till föreläggande att lämna upplysningar i syfte att underlätta husrannsakan i it-miljö bör införas i svensk rätt (avsnitt 8.3.4), samt ställningstagande till vilka förbehåll som bör avges såvitt avser insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter (avsnitt 8.3.5).

8.3.2 En möjlighet till skyndsamt bevarande av lagrade uppgifter i elektronisk form genom föreläggande införs

Förslag: Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott ska kunna föreläggas att bevara uppgiften. I föreläggandet ska anges under hur lång tid uppgiften ska bevaras. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga 90 dagar. Om det finns särskilda skäl ska tiden för bevarande få förlängas med högst 30 dagar.

Om det är möjligt ska föreläggandet ges skriftligt. I annat fall ska den som föreläggandet riktas mot så snart som möjligt få ett skriftligt bevis om beslutet. Meddelande om åtgärden får inte obehörigen föras vidare. Föreläggandet ska innehålla en underrättelse om detta.

Bevarandeföreläggande får inte riktas mot den som skäligen kan misstänkas för brottet eller mot närstående till den misstänkte.

Beslut om bevarandeföreläggande får meddelas av undersökningsledaren eller åklagaren.

Den som ålagts ett bevarandeföreläggande får begära rättens prövning av det. För rättens prövning ska i tillämpliga delar gälla vad som gäller för prövning av beslag.

Om ett bevarandeföreläggande riktas mot en sådan leverantör som är skyldig att lagra trafikuppgifter enligt lagen om elektronisk kommunikation ska samma regler som gäller i fråga om åtgärder för att skydda uppgifter som ska lagras, gälla även

för uppgift som omfattas av föreläggandet. Vidare ska motsvarande regler om rätt till ersättning för kostnader och om anpassning för utlämnande av uppgifter som gäller för lagring av trafikuppgifter gälla för uppgifter som ska bevaras.

Förslaget om skyndsamt bevarande av lagrade uppgifter medför även andra följdändringar i lagen om elektronisk kommunikation.

Skälen för förslaget

Inledande aspekter på en ny reglering

Artikel 16 i konventionen innebär att det ska vara möjligt att skyndsamt säkra särskilt angivna lagrade datorbehandlingsbara uppgifter. Ett säkrande innebär att uppgifterna ska bevaras på ett betryggande sätt. Med uppgifter avses vilken typ av uppgifter som helst, dvs. såväl trafik-, innehålls- som abonnentuppgifter. Den grundläggande tanken bakom artikeln är att säkrandet ska göras på ett mindre ingripande sätt än genom exempelvis husrannsakan och beslag. Säkrandet är vidare tänkt att kunna ske såväl hos fysiska som juridiska personer, inklusive tjänsteleverantörer.

Säkrandet enligt artikel 16 ska, mot bakgrund av artikel 14.2, kunna tillämpas såväl på de brott som straffbeläggs i enlighet med konventionen och på andra brott som begåtts med hjälp av ett datorsystem som generellt på insamling av bevis i elektronisk form om ett brott.

Vi har i avsnitt 5.4.4 gjort bedömningen att det krävs lagstiftning för att uppfylla de krav som ställs i artikel 16, eftersom de svenska bestämmelserna om operatörers lagringsskyldighet enligt LEK, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, husrannsakan och beslag samt editionsföreläggande inte ger tillräckliga möjligheter att säkra uppgifter på det sätt som konventionen föreskriver. Vi har vidare konstaterat att om det i svensk rätt inte införs någon möjlighet till säkrande av uppgifter på annat snabbare och mindre ingripande sätt än genom de medel som för närvarande står till buds innebär detta att inte heller konventionens bestämmelser om ömsesidig rättslig hjälp uppfylls.

I sammanhanget bör nämnas att polis och åklagare är av uppfattningen att det även i svensk rätt finns ett behov av en sådan möj-

lighet till snabbt säkrande av elektroniska uppgifter som avses i artikel 16. Vi delar den uppfattningen. Det finns alltså vid sidan av vad som krävs för ett konventionstillträde skäl att införa en form av föreläggande för att säkra elektroniska uppgifter.

Syftet med artikel 16 är att under en begränsad tidsperiod *säkra* datorbehandlingsbara uppgifter som *redan finns lagrade*. Syftet är således inte att skapa någon ny förpliktelse att lagra eller att lämna ut uppgifter. De brottsbekämpande myndigheternas tillgång till de uppgifter som säkrats är en från frågan om säkrande skild fråga som kan vara omgärdad av andra regler och förutsättningar än vad som gäller för säkrandet.

Mot denna bakgrund är det vår uppfattning att det säkrande som artikel 16 avser att få till stånd knappast innebär något intrång i enskildas integritet, även om det innebär visst tvång för den enskilde. Det är således inte fråga om sådan övervakning eller kartläggning av den enskildes personliga förhållanden som avses i 2 kap. 6 § andra stycket regeringsformen. Eftersom ett säkrande inte i sig innebär att några uppgifter ska lämnas ut är det inte heller fråga om intrång i rätten till korrespondens enligt artikel 8 i Europakonventionen. Det är egentligen först vid ett utlämnande av uppgifterna som skyddet mot intrång i den personliga integriteten gör sig gällande.

I sammanhanget bör också framhållas att de medel för säkrande som för närvarande står till buds i svensk rätt, och som innebär att de brottsbekämpande myndigheterna samtidigt får tillgång till uppgifterna, dvs. husrannsakan, edition och beslag liksom de hemliga tvångsmedlen, för den enskilde är långt mer ingripande och integritetskränkande än ett föreläggande om säkrande. Tanken bakom konventionens reglering i denna del är också att det ska införas ett sätt att bevara uppgifter i den nationella rätten som är mindre ingripande för de inblandade än husrannsakan och beslag.

Det kan vidare nämnas att Norge i samband med konventionstillträdet införde 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 ska gälla för viss tid, högst 90 dagar, men kan förlängas. Om säkrandet sker på begäran av annan stat ska det gälla i minst 60 dagar.

Att i svensk rätt införa en möjlighet till den typ av föreläggande som avses i artikel 16 ger samtidigt myndigheterna större möjligheter att välja det medel som är bäst anpassat till det enskilda fallet

och kan därmed leda till att den enskilde drabbas av ett lindrigare ingrepp i sin personliga integritet än vad som hade varit fallet om enbart nuvarande tvångsmedel för säkrande av uppgifter stod till buds.

Mot bakgrund av det anförda föreslår vi att det i svensk rätt införs en möjlighet att förelägga någon att under viss tid bevara lagrade elektroniska uppgifter som innehas av denne. Föreläggandet bör ha en generell utformning och kunna riktas mot såväl fysiska som juridiska personer och mot leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Även om konsekvenserna inte kan bedömas som särskilt ingripande, bör åtgärden betraktas som ett straffprocessuellt tvångsmedel. Den naturliga platsen för en sådan bestämmelse är 27 kap. rättegångsbalken.

I det följande redogör vi för hur de nya bestämmelserna om bevarande bör utformas.

Förutsättningar för ett föreläggande om bevarande av elektroniska uppgifter

Det är alltså vår uppfattning att det bör införas en möjlighet i svensk rätt att förelägga den som innehar lagrade uppgifter i elektronisk form att bevara uppgifterna under viss tid. Syftet med regleringen är att ge de brottsbekämpande myndigheterna en möjlighet att snabbt se till att elektroniska uppgifter som finns lagrade hos någon kan bevaras på ett för samtliga inblandade smidigare och mindre ingripande sätt än vad nuvarande tvångsmedel tillåter.

Det förtjänar på nytt att framhållas att den nya regleringen enbart tar sikte på ett betryggande bevarande av redan befintliga lagrade uppgifter. Lagrade elektroniska uppgifter som någon innehar ska alltså bevaras och behållas intakta under viss tid, i avvaktan på att de brottsbekämpande myndigheterna vidtar ytterligare åtgärder som är tillåtna enligt svensk lagstiftning för att få tillgång till uppgifterna, dvs. tar bevisningen i beslag, begär editionsföreläggande eller begär tillstånd till hemlig övervakning eller hemlig avlyssning av elektronisk kommunikation. De brottsbekämpande myndigheternas tillgång till uppgifterna som säkrats är således en annan fråga som inte direkt berörs av den nya regleringen. Regleringen innebär inte heller att någon ska kunna föreläggas att

framöver lagra uppgifter som ännu inte existerar. Föreläggande ska alltså inte kunna användas för att i realtid samla in uppgifter.

De elektroniska uppgifter som ska kunna bevaras genom ett föreläggande kan vara av vilket slag som helst. Det kan således exempelvis röra sig om att bevara en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat.

Den mot vilken föreläggandet riktar sig ska inneha de lagrade uppgifterna, vilket innebär att uppgifterna antingen ska finnas lagrade hos personen eller på annat sätt vara under den personens kontroll och åtkomst. Uppgifterna kan alltså finnas lagrade på en server någon annanstans än där personen fysiskt befinner sig, men ändå finnas tillgängliga för honom eller henne. Lagrade uppgifter kan innehas av flera olika personer samtidigt. Bevarandeföreläggande kan då riktas mot envar av dem. Så kan exempelvis vara fallet om en person har sin e-post lagrad på en server hos en annan person. Bevarandeföreläggande kan då riktas såväl mot den person hos vilken uppgifterna finns (dvs. den som innehar servern) som den person som på distans har kontroll över och åtkomst till uppgifterna (dvs. den person som innehar e-postkontot).

Något hinder mot att ge en person som befinner sig i Sverige föreläggande om bevarande bör inte finnas även om uppgifterna som ska bevaras finns lagrade på en server utomlands, så länge uppgifterna finns tillgängliga från Sverige för den som föreläggandet riktar sig mot. En annan sak är att det i ett senare skede, i samband med att de uppgifter som bevarats ska lämnas ut, i vissa situationer kan krävas rättslig hjälp av den stat där den server står som uppgifterna är lagrade på. Den som beslutar om föreläggande behöver således inte redan i samband med att föreläggande meddelas ha klart för sig exakt var uppgifterna som ska bevaras finns lagrade. Enligt vår mening kommer detta förhållningssätt inte i konflikt med folkrättsliga regler, eftersom ett bevarandeföreläggande enbart innebär att uppgifter som redan finns lagrade på ett visst ställe fortsatt ska bevaras. Ett annat synsätt skulle innebära att åtgärden att ge ett bevarandeföreläggande skulle bli mindre verksamt i praktiken. I den situationen att den som har vissa lagrade elektroniska uppgifter under sin kontroll och åtkomst befinner sig i Sverige, medan uppgifterna är lagrade på en server utomlands är det naturligt att rikta bevarandeföreläggandet mot den som befinner sig i Sverige. Det kan vara i det närmaste praktiskt ogörligt att i den

situationen få till stånd rättslig hjälp med ett skyndsamt säkrande av uppgifterna i den stat där servern befinner sig.

Ett säkrande av elektroniska uppgifter bör kunna göras i ett tidigt skede av en brottsutredning. Ett bevarandeföreläggande bör kunna regleras efter samma former som beslag. Något krav på att förundersökningen har kommit så långt att någon är skäligen misstänkt för brottet bör därför inte uppställas. För att föreläggande ska få användas bör därför räcka att någon innehar viss lagrad uppgift i elektronisk form som skäligen kan antas ha betydelse för utredningen om ett brott. För det fall det dock finns en skäligen misstänkt person bör föreläggande inte kunna riktas mot honom eller henne. Inte heller bör ett föreläggande kunna riktas mot den misstänktes närstående.

Som vi tidigare har konstaterat, kan en säkrandeåtgärd av det slag som nu föreslås, inte i sig anses ingripande ur integritetssynpunkt. Säkrande bör, som nämnts, kunna komma till stånd i ett tidigt skede av en brottsutredning, då det inte alltid säkert kan fastställas exakt hur allvarligt det aktuella brottet är.

Enligt artikel 14.2 ska de åtgärder som avses i artikel 16 kunna tillämpas på de brott som straffbeläggs i enlighet med konventionen och på andra brott som begåtts med hjälp av ett datorsystem samt generellt på insamling av bevis i elektronisk form om ett brott. Även om det enligt konventionen förutsätts en generell möjlighet till säkringsåtgärder, är det dock möjligt att i den nationella lagstiftningen närmare reglera vilka förutsättningar som ska vara uppfyllda för att åtgärderna ska få vidtas.

Vi anser att något krav på det aktuella brottets svårhetsgrad inte bör ställas upp. Som framgått är det i ett tidigt skede av utredningen inte alltid möjligt att avgöra brottets svårhet. I detta skede finns det inte någon anledning att ställa upp några särskilda krav för åtgärden. Sådana krav aktualiseras i stället när fråga uppkommer om ett röjande av uppgifterna. Föreläggande att bevara elektroniska uppgifter bör alltså få användas oavsett brottets svårhetsgrad. Inte heller när det gäller beslag uppställs något krav på att brottet ska vara av viss svårhet (se 27 kap. 1 § rättegångsbalken).

Vid beslut om och användning av tvångsmedel gäller dock generellt proportionalitetsprincipen, vilken innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med den (se t.ex. prop. 2011/12:55 s. 72). Proportionalitetsprincipen kommer att gälla även när det

gäller föreläggande att bevara elektroniska uppgifter. Principen finns uttryckt i 27 kap. 1 § tredje stycket rättegångsbalken.

Av proportionalitetsprincipen följer att de brottsbekämpande myndigheterna inte ska meddela ett bevarandeföreläggande om de redan då de överväger att meddela föreläggandet kan se att det, mot bakgrund av brottets svårhet eller av andra skäl, inte finns någon möjlighet att med stöd av de regler som gäller för detta, senare få ut de uppgifter som skulle säkras. Så skulle kunna vara fallet om de brottsbekämpande myndigheterna vet om att uppgifterna finns lagrade på en server utomlands, att det kommer att krävas rättslig hjälp från den stat där servern står för att i ett senare skede få tillgång uppgifterna och att sådan rättslig hjälp inte kommer att kunna beviljas.

Innebörden av ett föreläggande om bevarande av lagrade elektroniska uppgifter

Ett föreläggande om bevarande av elektroniska uppgifter går alltså ut på att vissa särskilt angivna lagrade elektroniska uppgifter under viss tid ska behållas intakta och bevaras på ett sådant sätt att de under denna tid inte kan förstöras, förändras eller på annat sätt göras oåtkomliga. En begränsning ligger i att uppgiften måste finnas lagrad och att den måste innehas av den som föreläggandet riktar sig mot.

Ytterligare en begränsning ligger i att föreläggandet ska avse ”en viss” elektronisk uppgift. I föreläggandet måste således anges vilken specifik elektronisk uppgift som ska bevaras, exempelvis en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan alltså inte tillåtas vara generellt i den meningen att den som föreläggandet riktar sig mot exempelvis ska bevara alla uppgifter som mottagits under en viss tidsperiod.

Ett föreläggande om bevarande kan tänkas bli uppfyllt på olika sätt. Ett alternativ är att den som föreläggandet riktar sig mot kopierar uppgiften. Ett annat är att uppgiften lämnas orubbad på sin ursprungliga plats, samtidigt som åtgärder vidtas så att den inte kan raderas eller ändras på något sätt.

Det går knappast att i lag reglera på vilket sätt bevarandet ska göras, speciellt som ett föreläggande ska kunna rikta sig mot olika typer av aktörer. Vid behov bör den som har beslutat om föreläggandet, eventuellt i samråd med den som föreläggandet riktar sig

mot, ge anvisningar om hur uppgiften bör bevaras i det enskilda fallet för att bevarandeskyldigheten ska anses ha blivit uppfylld. Om föreläggandet riktar sig mot en enskild person kan det vara av större vikt att det ges tydliga instruktioner för på vilket sätt personen ska följa föreläggandet än om föreläggandet riktar sig mot en sådan operatör som omfattas av regleringen i LEK, vilken har erfarenhet och vana av samarbete med de brottsbekämpande myndigheterna i frågor rörande säkrande av elektronisk bevisning. Det bör dock framhållas att bevarandet av uppgifterna sker på den förelagdes risk, och att den personen har att se till att uppgifterna behålls intakta under den avsedda tidsperioden. Detta innebär även att om den förelagde inte skulle följa eventuella anvisningar om på vilket sätt uppgifterna bör bevaras, föreläggandet måste anses ha uppfyllts om uppgifterna finns intakta i samband med att de i ett senare skede begärs utlämnade.

De elektroniska uppgifterna ska bevaras under viss närmare angiven tid. I artikel 16.2 anges att uppgifterna ska bevaras så länge som behövs, dock högst 90 dagar. En fördragsslutande stat får dock införa en möjlighet att förnya föreläggandet. I konventionens bestämmelser om ömsesidig rättslig hjälp med provisoriska åtgärder, anges i artikel 29.7 att ett säkrande av uppgifter som verkställts på begäran av en annan fördragsslutande stat ska gälla under en period om minst 60 dagar, för att den ansökande staten ska ha möjlighet att komma in med en begäran om utlämnande av uppgifterna. Sedan en framställning om utlämnande kommit in, ska uppgifterna bevaras i avvaktan på ett beslut om framställningen ska bifallas eller inte.

Mot den angivna bakgrunden anser vi att den längsta förelagda tiden för bevarande bör vara 90 dagar. Tiden för bevarande bör dock aldrig vara längre än nödvändigt i det enskilda fallet. Enligt vår uppfattning måste den maximala tiden för bevarande, 90 dagar, i de flesta fall vara en fullt tillräcklig tid för att de brottsutredande myndigheterna ska kunna komma fram till om de ska vidta åtgärder för att få tillgång till uppgifterna. I de fall då en begäran om säkrande inkommer från en annan stat, kan det dock i vissa mer komplicerade fall krävas längre tid för bevarande än 90 dagar. Det kan även i andra fall krävas att uppgifterna bevaras under längre tid än 90 dagar, även om det torde vara sällsynt. Vi föreslår mot den bakgrunden att det ska vara möjligt att förlänga den ursprungliga tiden för bevarande med högst 30 dagar om det finns särskilda skäl för det.

Enligt artikel 16.3 ska den som ett föreläggande om bevarande riktas mot, åläggas att hemlighålla att åtgärder för säkrande av uppgifter vidtagits. Även ur ett allmänt brottsbekämpningsperspektiv framstår det som naturligt att den som ska bevara uppgifterna åläggs en sådan tystnadsplikt. I annat fall finns risk för att förundersökningen äventyras. I sammanhanget kan nämnas att tystnadsplikt med stöd av befintliga regler kan åläggas någon i samband med andra åtgärder under förundersökningsförfarandet. Enligt 23 kap. 10 § sista stycket rättegångsbalken får undersökningsledaren besluta att det som förekommit vid förhör inte får uppenbaras och om det vid en domstolsförhandling inom stängda dörrar lagts fram exempelvis uppgifter för vilka förundersökningssekretess gäller får rätten enligt 5 kap. 4 § rättegångsbalken besluta att uppgiften inte får uppenbaras. För det fall något annat inte meddelats, bör därför den som föreläggandet riktar sig mot vara skyldig att hemlighålla att säkrande åtgärder vidtagits. Vi föreslår därför att det uttryckligen ska föreskrivas att den som ett bevarandeföreläggande riktar sig mot inte obehörigen ska få föra vidare att säkrande åtgärder har vidtagits. Ett föreläggande om bevarande bör innehålla en underrättelse om detta.

Beslutsbefogenheten m.m.

Ett föreläggande om bevarande av viss elektronisk uppgift bör som sagts meddelas skyndsamt och i ett tidigt skede av förundersökningen. Praktiska skäl talar för att annan än domstol bör besluta om föreläggande.

Vi har tidigare konstaterat att ett föreläggande om bevarande, mot bakgrund av att det enbart handlar om att säkra uppgifter, inte kan anses särskilt känsligt ur integritetssynpunkt.

Det finns därför inte heller av hänsyn till rättssäkerheten skäl att lägga beslutsbefogenheten på domstol.

Ett föreläggande måste kunna meddelas snabbt så att viktig framtida bevisning inte går förlorad. Det skulle därför kunna övervägas om beslutanderätt borde tillkomma var och en som kan besluta om beslag, dvs. åklagare eller annan förundersökningsledare och, i brådskande fall, polisman (jfr 27 kap. 4 § andra stycket rättegångsbalken). Det är emellertid fråga om en ny typ av åtgärd vars användande inbegriper en del juridiska överväganden. Detta talar för att beslutanderätten bör tillkomma enbart åklagare. Om det

uppkommer en fråga om att meddela ett föreläggande under en förundersökning som leds av polisen framstår det dock, mot bakgrund av att ett föreläggande inte kan anses så känsligt ur integritetssynpunkt, som omotiverat att enbart detta föranleder att en åklagare tar över förundersökningen i ett tidigare skede än som annars skulle ha varit fallet. Ett bevarandeföreläggande bör därför enligt vår mening kunna meddelas såväl av åklagare som av annan förundersökningsledare. Om såväl åklagare som annan förundersökningsledare får besluta om bevarandeföreläggande, framstår det praktiska behovet av att låta även en polisman besluta om föreläggande som litet. Till skillnad från när det gäller olika situationer där det finns behov av att ta föremål i beslag, är det nämligen svårt att tänka sig situationer då ett bevarandeföreläggande måste meddelas så skyndsamt att ett beslut från åklagare eller annan undersökningsledare inte kan inväntas. Enbart åklagare eller annan undersökningsledare bör därför få besluta om bevarandeföreläggande.

I de fall Tullverket, med stöd av 19 § lagen (2000:1225) om straff för smuggling (smugglingslagen) inlett förundersökning kommer även Tullverket, så länge förundersökningen leds av befattningshavare vid Tullverket, ha möjlighet att besluta om bevarandeföreläggande, eftersom de befogenheter och skyldigheter som undersökningsledaren har enligt rättegångsbalken i sådant fall gäller Tullverket (se 19 § smugglingslagen). Det kan exempelvis gälla vid in- och utförsel av barnpornografi eller vid smuggling av narkotika och alkohol. Eftersom ledningen av förundersökningen enligt 19 § smugglingslagen emellertid ska övertas av åklagaren så snart någon skäligen kan misstänkas för brottet om saken inte av enkel beskaffenhet och åklagaren även annars ska överta ledningen, när detta är påkallat av särskilda skäl, bör det i praktiken bli få fall där Tullverket kommer att besluta om bevarandeföreläggande.

Det är av vikt att omfattningen av ett bevarandeföreläggande tydligt framgår. Enligt vår mening bör ett bevarandeföreläggande som huvudregel därför ges i skriftlig form. Det kan emellertid tänkas uppstå situationer då det finns ett behov av att meddela ett bevarandeföreläggande muntligt, exempelvis om ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande. En möjlighet att ge föreläggande muntligt bör därför finnas. I det fallet bör den förelagde emellertid, så snart som möjligt, få ett skriftligt bevis om beslutet. Ett huvudskäl till detta är, som nämnts, att föreläggandets omfattning måste vara klart och att den förelagde måste veta vilken elektronisk uppgift som avses.

Ett annat viktigt skäl är att beslutet behövs för att den förelagde ska kunna få detta prövat av domstol (se i det följande). Beslutet ska därför innehålla uppgift om vilken domstol som i förekommande fall ska pröva frågan. Som tidigare nämnts bör ett föreläggande om bevarande också innehålla en underrättelse om att den som föreläggandet riktar sig mot är skyldig att hemlighålla att säkrande åtgärder vidtagits.

Sanktioner

Om den som förelagts att bevara viss lagrad elektronisk uppgift skulle välja att inte följa föreläggandet, är frågan om något straffansvar kan eller bör utkrävas. Det bör framhållas att konventionen inte kräver att det införs några sanktioner mot den som inte följer ett sådant föreläggande om att säkra uppgifter som avses i artikel 16. Det bör vidare noteras att ett föreläggande om bevarande inte kan eller är tänkt att användas i syfte att förhindra att uppgifter försvinner på grund av att den som förvarar uppgifterna är opålitlig. I sådana fall finns skäl att säkra uppgifterna på andra mer ingripande sätt, exempelvis genom husrannsakan och beslag. De personer som ett bevarandeföreläggande i första hand är avsett att riktas mot är alltså sådana som kan förväntas följa det enbart på grund av föreläggandet som sådant, och inte på grund av att de riskerar sanktioner om det inte följs.

Den straffbestämmelse som skulle kunna komma i fråga att tillämpa är bestämmelsen i 17 kap. 13 § brottsbalken om överträdelse av myndighets bud.

Bestämmelsens första stycke upptar gärningar som innebär att någon på olika sätt motverkar en myndighets åtgärd. Stycket kan sägas omfatta fyra olika typsituationer (se Berggren m.fl., *Brottsbalken En kommentar kap. 13–24*, s. 17:60). Straffet är böter eller fängelse i högst ett år för den som olovligen

1. rubbar, skadar eller annars förfogar över egendom som är föremål för utmätning, kvarstad, betalningssäkring, beslag eller annan liknande åtgärd,
2. skadar eller borttager myndighets anslag eller försegling,
3. öppnar vad myndighet tillslutit, eller
4. överträder annat dylikt av myndighet meddelat förbud.

Gärningarna under punkten 1 innebär alltså att reglerna i vissa rättsinstitut är straffsanktionerade om förbudet överträds genom en sådan gärning som anges i bestämmelsen (se Berggren m.fl., *Brottsbalken En kommentar kap. 13–24*, s. 17:60). Rättsinstituten är utmätning, kvarstad, betalningssäkring, beslag eller *annan liknande åtgärd*. I uttrycket ”annan liknande åtgärd” inbegrips, enligt departementschefen i prop. 1980/81:84 (s. 215–216) införsel och verkställighet enligt 16 kap. utsökningsbalken samt verkställighet som kan förekomma utanför utsökningsbalkens område, och därför även verkställighet genom en administrativ myndighets försorg, dock endast om åtgärden avser viss egendom. Vidare inbegrips, enligt departementschefen, en åtgärd som i likhet med de nyss nämnda vidtas av en myndighet och innefattar ett rättsligt ingripande i syfte att begränsa rådigheten beträffande viss egendom. Enligt departementschefen omfattar bestämmelsen inte bara att någon handlar i strid mot ett förbud som myndigheten uttryckligen meddelar utan även att någon bryter mot ett förbud som enligt lag följer av ett visst beslut (t.ex. om utmätning).

Otillåtna förfoganden blir straffbara så snart beslutet träder i kraft (prop. 1980/81:84 s. 217). Det förutsätts alltså inte att beslutet har kommit till uttryck genom märkning eller annat säkerställande av den egendom som är föremål för ingripandet. Endast uppsåtligt handlande är emellertid straffbelagt. Ansvar kommer alltså bara i fråga för den som känner till beslutet.

Som framgått straffbeläggs även *överträdelse av annat dylikt myndighets förbud*. Med detta avses fall som kan anses som helt likvärdiga med de åtgärder som uttryckligen har angetts i bestämmelsen (Berggren m.fl., *Brottsbalken En kommentar kap. 13–24*, s. 17:63). Som exempel kan nämnas de i 27 kap. 15 § rättegångsbalken angivna åtgärderna att för säkerställande av utredning om brott tillstänga byggnad eller rum, förbjuda tillträde till visst område, meddela förbud mot flyttande av visst föremål eller vidta annan dylik åtgärd (NJA II 1948 s. 338 och Berggren m.fl., *Brottsbalken En kommentar kap. 13–24*, s. 17:63).

Det finns enligt vår mening inte något som talar emot att bestämmelsen åtminstone i vissa situationer även skulle vara tillämplig på otillåtna åtgärder med elektroniska uppgifter.

Vårt förslag i fråga om skyndsamt bevarande av uppgifter i elektronisk form innebär att den som innehar viss lagrad uppgift i elektronisk form som skäligen kan antas ha betydelse för utredning om ett brott ska kunna *föreläggas att bevara* uppgiften under viss tid.

Bestämmelsen är alltså inte utformad som en möjlighet för en myndighet att *meddela förbud mot att rubba* elektroniska uppgifter. Genom föreläggandet åläggs en enskild person att vidta en aktiv åtgärd – att bevara – och inte att enbart avstå från något – att inte rubba. Enligt vår mening är det nödvändigt att utforma föreläggandet på detta sätt, dvs. att den som föreläggandet riktar sig mot aktivt ska säkra uppgiften och inte enbart åläggs att inte rubba den. I annat fall finns risk för att uppgiften går förlorad trots att föreläggandet följs, exempelvis om det företag som föreläggandet riktar sig mot har som praxis att radera vissa uppgifter automatiskt efter viss tid. Mot bakgrund av hur förslaget till föreläggande alltså är utformat är det inte alldeles säkert att den som underlåter att följa ett bevarandeföreläggande alltid kan hållas straffrättsligt ansvarig enligt bestämmelsen i 17 kap. 13 § brottsbalken. Ett föreläggande att bevara en uppgift innebär dock samtidigt även ett förbud mot att exempelvis radera uppgiften. Vår tolkning är att bestämmelsen därför skulle kunna vara tillämplig, i vart fall i vissa situationer.

Det skulle i och för sig vara möjligt att göra en ändring i 17 kap. 13 § brottsbalken, så att den som inte följer ett bevarandeföreläggande med all säkerhet träffas av bestämmelsen, alternativt att införa en särskild straffbestämmelse. Samtidigt är det tveksamt om det finns tillräckliga skäl att införa en ny sådan bestämmelse som enbart tar sikte på dessa fall. Som vi redan berört är bedömningen att redan existensen av ett föreläggande oftast kommer att vara tillräckligt. Det framstår därför som lämpligare att låta rättspraxis och utvecklingen i övrigt avgöra i vilken utsträckning utökade eller nya straffrättsliga sanktioner behövs.

Den som utan giltigt skäl röjer vad som enligt rättens eller undersökningsledarens förordnande inte får uppenbaras döms, enligt 9 kap. 6 § rättegångsbalken, till böter. Straffansvar enligt den bestämmelsen kommer att kunna utkrävas för den som utan tillstånd eller giltigt skäl bryter mot skyldigheten att hemlighålla att säkringsåtgärder vidtagits enligt den föreslagna nya bestämmelsen.

Rättens prövning

Ett föreläggande om bevarande av viss lagrad uppgift i elektronisk form innebär att en fysisk eller juridisk person åläggs en skyldighet att under viss tid bevara bestämda uppgifter som denne innehar i elektronisk form. Tiden för bevarande får inte bestämmas längre än

nödvändigt och får maximalt bestämmas till 90 dagar, med möjlighet till 30 dagars förlängning om det finns särskilda skäl för det.

Ett föreläggande om bevarande innebär ett visst ingrepp mot den enskilde. Det är emellertid fråga om ett begränsat integritetsintrång och föreläggandet kan inte anses innebära något intrång i rätten till korrespondens enligt artikel 8 i Europakonventionen. Det kan vidare förutsättas att tidsperioden för bevarande i de allra flesta fall kommer att bli relativt kort. Detta talar för att det inte är behövligt att låta ett föreläggande om bevarande kunna bli föremål för rättens prövning.

Samtidigt kan inte uteslutas att den maximala tidsperioden för bevarande i vissa fall kan behöva utnyttjas. Om ett bevarandeföreläggande inte följs bör, som vi nyss har berört, straffansvar enligt gällande regler kunna komma i fråga i vissa fall. Den som föreläggandet riktar sig mot är vidare under straffansvar ålagd tystnadsplikt i fråga om att säkrande åtgärder vidtagits. Mot den bakgrunden anser vi att den som ålagts ett föreläggande enligt den föreslagna nya bestämmelsen bör ha möjlighet att begära rättens prövning av föreläggandet. Rätten bör pröva frågan tämligen omgående, så att den som ålagts föreläggandet får besked om vad han eller hon har att rätta sig efter framöver. Skulle någon tidsfrist för prövningen inte ställas upp, finns risk för att den tid för bevarande som ställts upp i föreläggandet hinner gå till ända innan rätten har hunnit pröva frågan. Enligt vår mening är det mot den bakgrunden lämpligt att knyta an till de regler i 27 kap. 6 § rättegångsbalken som gäller för rättens prövning av ett beslag. Den som ålagts ett föreläggande har då möjlighet att begära rättens prövning av föreläggandet, varvid rätten ska hålla förhandling så snart som möjligt och, om det inte finns något synnerligt hinder mot det, senast fjärde dagen efter det att begäran om prövning har kommit in.

Som framgått föreslår vi att det uttryckligen ska föreskrivas att den som ett bevarandeföreläggande riktar sig mot inte obehörigen ska få föra vidare att säkrande åtgärder har vidtagits.

Enligt 18 kap. 1 § offentlighets- och sekretesslagen (2009:400) gäller sekretess bl.a. för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet som avser förebyggande av brott, om det kan antas att syftet med beslutade åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretessen följer med uppgiften när den lämnas vidare till en annan myndighet och gäller hos alla myndigheter som tar befattning med

tvångsåtgärder, t.ex. en domstol som prövar ett bevarandeföreläggande. En sekretessbestämmelse som gäller för en uppgift i ett mål eller ett ärende i en domstols rättskipande eller rättsvårdande verksamhet upphör enligt 43 kap. 8 § första stycket offentlighets- och sekretesslagen att vara tillämplig om uppgiften tas in i en dom eller ett annat beslut i samma mål eller ärende. Domstolen kan enligt andra stycket förordna att sekretessbestämmelsen ska vara tillämplig även i fortsättningen. Ett sådant sekretessförordnande får dock enligt tredje stycket inte omfatta själva domslutet eller motsvarande del av annat beslut, såvida inte rikets säkerhet eller annat intresse av synnerlig vikt oundgängligen påkallar det. Föreskriften i styckets sista mening om att detta, bl.a. för mål eller ärenden som rör anklagelse för brott, endast gäller om riket befinner sig i krig eller motsvarande är inte tillämplig på förfaranden rörande hemlig avlyssning av elektronisk kommunikation eller andra hemliga tvångsmedel eftersom sådana förfaranden inte omfattas av uttrycket ”anklagelse mot någon för brott” (se NJA 2011 not N 28, jfr prop. 2003/04:93 s. 66–67 med hänvisningar). Inte heller bevarandeföreläggande kan anses omfattas av uttrycket ”anklagelse mot någon för brott”.

Rekvisitet ”såvida inte […] annat intresse av synnerlig vikt oundgängligen påkallar det” i 43 kap. 8 § tredje stycket offentlighets- och sekretesslagen anses i allmänhet uppfyllt när det gäller beslut om hemliga tvångsmedel (se NJA 2011 not N 28 med hänvisningar). Enligt vår uppfattning skulle i vissa fall rekvisitet även kunna vara uppfyllt när det gäller beslut om bevarandeföreläggande. I så fall ska rätten, när den beslutar om bevarandeföreläggandet ska bestå, ta in förordnande om att sekretessbestämmelsen i 18 kap. 1 § offentlighets- och sekretesslagen ska vara tillämplig även i fortsättningen i själva beslutet om att bevarandeföreläggandet ska bestå eller upphävas. I annat fall blir uppgifterna i beslutet offentliga.

För den som bevarandeföreläggandet riktats mot är det som nyss har sagts av följande betydelse. Om rätten förordnar att sekretessbestämmelsen i 18 kap. 1 § offentlighets- och sekretesslagen ska vara tillämplig även i fortsättningen gäller en vittomfattande tystnadsplikt om att säkrande åtgärder vidtagits även framöver. I annat fall kan den som föreläggandet riktar sig mot inte anses ha tystnadsplikt i fråga om sådana uppgifter som kan utläsas ur rättens offentliga beslut. Att röja uppgifter som framgår av ett offentligt domstolsbeslut innebär inte att något obehörigen förs vidare. Straffansvar enligt 9 kap. 6 § rättegångsbalken kan alltså inte inträda i detta fall. Hur omfattande tystnadsplikten är i den situationen att uppgifterna i

domstolens beslut blir offentliga beror således på hur rätten har utformat sitt beslut om att bevarandeföreläggandet ska bestå eller upphävas.

Rättens beslut kan överklagas av någon av parterna med stöd av 49 kap. 5 § 6 rättegångsbalken. Om rätten upphäver föreläggandet kan undersökningsledaren eller åklagaren enligt 52 kap. 7 § tredje stycket rättegångsbalken begära inhibition, i syfte att förhindra att bevisningen går förlorad innan överinstansen har hunnit ta ställning i frågan.

Det bör framhållas att bevarandeföreläggandet gäller fram till dess att rätten eller den som ursprungligen har meddelat föreläggandet meddelar något annat. Vidare bör framhållas att frågan om bevarandeföreläggandet ska bestå är en sak mellan den som ålagts föreläggandet och den som beslutat det. Om det finns en misstänkt person har han eller hon alltså inte någon rätt att närvara vid förhandlingen och ska inte underrättas om eller kallas till denna.

Behov av ändringar i lagen om elektronisk kommunikation

Till följd av förslaget om skyndsamt säkrande av lagrade uppgifter i elektronisk form genom bevarandeföreläggande bör vissa ändringar göras i 6 kap. LEK.

Som vi tidigare har redogjort för kräver konventionen att elektroniska uppgifter ska kunna säkras såväl hos fysiska som juridiska personer, inklusive tjänsteleverantörer. Ett bevarandeföreläggande måste alltså kunna riktas även mot den som är operatör och omfattas av regleringen i LEK.

Ett bevarandeföreläggande kan även avse sådana trafikuppgifter som ska lagras enligt 6 kap. 16 a § LEK. Enligt en nyligen framtagen utvärderingsrapport av den kommitté inom Europarådet som övervakar konventionen (the Cybercrime Convention Committee [T-CY]) är den lagringsskyldighet som följer av EU:s direktiv om lagring av trafikuppgifter och den möjlighet att säkra lagrade elektroniska uppgifter som ska finnas enligt konventionen avsedda att vara till varandra kompletterande medel för att få tillgång till bevisning i elektronisk form. De kan användas parallellt, i kombination eller separat i olika syften. En skyldighet att lagra vissa uppgifter innebär exempelvis, enligt rapporten, att det är större chans att historiska trafik- lokaliserings- eller abonnentuppgifter fortfarande finns tillgängliga i samband med att säkrande åtgärder vidtas. Om den gene-

rellt bestämda lagringstiden är på väg att gå till ända för vissa uppgifter och ett föreläggande om att säkra uppgifterna då meddelas, innebär detta också, framhålls i rapporten, att dessa finns bevarade även efter att den automatiska tiden för lagring gått ut och att uppgifterna därmed kan användas i en särskild brottsutredning (Assessment report, *Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, Version 14 November 2012, s. 73).

Ett bevarandeföreläggande riktat mot en operatör kan även avse andra uppgifter än trafikuppgifter, t.ex. innehållsuppgifter, under förutsättning att uppgiften finns lagrad hos operatören.

I samband med att skyldigheten att lagra trafikuppgifter infördes i LEK anförde regeringen att lagringen, för att ha den säkerhet som krävdes för att uppnå sitt syfte och för att skapa en hög tillit till systemet, måste utföras så att både integritetsskyddet och effektiviteten tillgodoseddes (prop. 2010/11:46 s. 51). Det tekniska såväl som det organisatoriska skyddet måste vara tillräckligt. Det fordrades enligt regeringens mening därför också en aktiv tillsynsverksamhet med en tillsynsmyndighet som hade god kännedom om regleringen av marknaden för elektronisk kommunikation och samtidigt insikter i hur trafikuppgifter fick användas i brottsbekämpningen. Mot den bakgrunden infördes en särskild bestämmelse i LEK (6 kap. 3 a §) om leverantörernas skyldighet att vidta särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de trafikuppgifter som lagrats för brottsbekämpande syften. Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om leverantörens skyldighet att vidta dessa åtgärder. Post- och telestyrelsen (PTS) har utsetts till tillsynsmyndighet för lagringen. Med stöd av 37 § förordningen (2003:396) om elektronisk kommunikation har PTS föreskrivit och utfärdat allmänna råd om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål (PTSFS 2012:4).

De uppgifter som omfattas av ett bevarandeläggande hos en operatör kan utgöra samma uppgifter som lagrats enligt 6 kap. 16 a § LEK. De kan också utgöras av andra uppgifter, exempelvis sådana innehållsuppgifter som enbart kan fås ut genom bestämmelserna om hemlig avlyssning av elektronisk kommunikation. Uppgifter som under viss tid ska bevaras av en operatör kan således vara av integritetskänslig karaktär. Utlämnandet av sådana uppgifter är omgärdat av särskilda regler. Mot den bakgrunden är det, även om det här inte är fråga om att lämna ut några uppgifter, viktigt att uppgifterna

bevaras på ett säkert sätt och att integritetsskyddet tillgodoses. Vi föreslår därför att den särskilda bestämmelsen om kvalitet och säkerhet när det gäller de trafikuppgifter som lagrats för brottsbekämpande syften i 6 kap. 3 a § LEK görs tillämplig även i de fall då någon som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § LEK förelagts att bevara viss lagrad uppgift enligt den nya bestämmelsen i rättegångsbalken. PTS kommer då att ha att utöva tillsyn även över operatörernas skyldighet att bevara uppgifter enligt rättegångsbalken och således exempelvis granska om operatörerna vidtar de särskilda tekniska och organisatoriska åtgärder som föreskrivits till skydd för uppgifterna.

Även de bestämmelser i 6 kap. LEK som gäller rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut (16 e §) och om anpassning för utlämnande av uppgifter (16 f §), bör gälla för uppgifter som omfattas av ett bevarandeföreläggande enligt den nya bestämmelsen i rättegångsbalken hos någon som är anmälningspliktig enligt 2 kap. 1 § LEK. Ersättning ska då betalas till den som bevarat uppgifterna av den myndighet som har begärt uppgifterna. Regeringen eller den myndighet som regeringen bestämmer ska då meddela föreskrifter om ersättning. Enligt 46 § förordningen (2003:396) om elektronisk kommunikation får PTS när det gäller ersättning för kostnader som uppstår när uppgifter som lagrats enligt 6 kap. 16 a § LEK lämnas ut meddela föreskrifter om ersättningen. Motsvarande bör gälla när det gäller ersättning i samband med att uppgifter som bevarats enligt 27 kap. 16 § rättegångsbalken lämnas ut.

Enligt 6 kap. 5 § LEK är den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § LEK som huvudregel skyldig att utplåna eller avidentifiera trafikuppgift när sådan uppgift inte längre behövs för att överföra ett elektroniskt meddelande. I bestämmelsen finns några undantag från huvudregeln, bl.a. när det gäller lagringsskyldigheten enligt 6 kap. 16 a § LEK. Undantag måste gälla även för uppgifter som ska bevaras enligt den nya bestämmelsen i rättegångsbalken.

I 6 kap. 16 d § LEK finns en skyldighet för lagringsskyldiga operatörer att efter sex månader utplåna uppgifter som lagrats, om uppgifterna inte inom denna tid begärts utlämnade. I bestämmelsen bör läggas till att uppgifter som ska bevaras enligt den föreslagna nya bestämmelsen i rättegångsbalken inte ska utplånas innan tiden för bevarande har löpt ut.

Enligt 6 kap. 21 § LEK har den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst tystnadsplikt för bl.a. uppgift som hänför sig till användning av vissa hemliga tvångsmedel. Tystnadsplikt bör gälla även för uppgift som hänför sig till föreläggande att bevara uppgift enligt den föreslagna nya bestämmelsen i rättegångsbalken.

8.3.3 En skyldighet för leverantörer att lämna ut uppgift om andra leverantörer införs

Förslag: Det införs en skyldighet för leverantörer att till den myndighet som beslutat om ett bevarandeföreläggande lämna ut uppgift om vilka övriga leverantörer som har deltagit vid överföringen av det meddelande som omfattas av föreläggandet. Förslaget medför även vissa följdändringar.

Skälen för förslaget

I föregående avsnitt har vi, för att svensk rätt ska uppfylla de krav på skyndsamt säkrande av lagrade uppgifter som ställs i artikel 16 i konventionen, föreslagit att en möjlighet införs att förelägga någon som innehar viss lagrad uppgift i elektronisk form som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften. Enligt artikel 17 ska ett sådant skyndsamt säkrande av trafikuppgifter som avses i artikel 16 kunna äga rum oavsett om en eller flera tjänsteleverantörer har varit inblandade vid överföringen av ett meddelande.

Som tidigare angetts är i många fall flera tjänsteleverantörer involverade då elektroniska uppgifter överförs. Det är därför inte säkert att det är tillräckligt att trafikuppgifter hos enbart en av tjänsteleverantörerna i överföringskedjan säkras. För att det ska vara möjligt att förelägga samtliga de tjänsteleverantörer som deltagit vid överföringen att bevara trafikuppgifter krävs först att dessa kan identifieras.

För att säkrande ska kunna äga rum hos de tjänsteleverantörer som varit delaktiga vid överföringen föreskriver artikel 17 att det ska vara möjligt att skyndsamt få tillgång till de uppgifter som krävs för att tjänsteleverantörerna och den väg på vilken meddelandet överfördes ska kunna spåras.

Säkrandet enligt artikel 17 ska, mot bakgrund av artikel 14.2, kunna tillämpas såväl på de brott som straffbeläggs i enlighet med konventionen och på andra brott som begåtts med hjälp av ett datorsystem som generellt på insamling av bevis i elektronisk form om ett brott.

Vi har i avsnitt 5.4.5 gjort bedömningen att det krävs lagstiftning för att uppfylla de krav som ställs i artikel 17.

När det gäller det skyndsamma utlämnande av uppgifter som regleras i artikel 17, handlar det om ett ytterst begränsat uppgiftsutlämnande där det enda syftet är att få klarhet i *vilka tjänsteleverantörer* som deltagit vid överföringen så att ett *säkrande* av uppgifter kan komma till stånd hos övriga tjänsteleverantörer.

Eftersom det handlar om utlämnande av uppgifter som behövs för att kunna identifiera vilka tjänsteleverantörer som deltagit vid överföringen är det i praktiken enbart leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster som berörs av en eventuell ny sådan reglering. Mot den bakgrunden är frågan om en ny bestämmelse om utlämnande av sådana uppgifter bör placeras i rättegångsbalken eller i LEK.

Fram till den 1 juli 2012 kunde de brottsutredande myndigheterna få tillgång till historiska uppgifter om meddelanden i ett elektroniskt kommunikationsnät (med dåvarande terminologi telemeddelanden) både enligt rättegångsbalkens regler om hemlig övervakning av elektronisk kommunikation (då benämnt hemlig teleövervakning) och genom utlämnande direkt från leverantörerna enligt LEK. Det var samma slags uppgifter som avsågs i de båda regelverken. Det kunde vara fråga om uppgifter om meddelandets ursprung, destination, färdväg, datum, tid, storlek eller varaktighet eller typ av tjänst.

Förutsättningarna för att kunna utnyttja de båda regelverken skilde sig åt. Ett utlämnande enligt LEK krävde att det var fråga om misstanke om brott med lägst fängelse i två år i straffskalan, vilket skulle jämföras med kravet på minst sex månaders fängelse vid hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken. I detta hänseende var alltså kravet i LEK strängare än i rättegångsbalken. LEK saknade däremot motsvarigheter till rättegångsbalkens övriga krav. LEK ställde alltså inte upp krav på att det skulle finnas en skäligen misstänkt person för brottet, att åtgärden skulle bedömas vara av synnerlig vikt för utredningen, att åtgärden enbart fick avse vissa adresser och nät, att åtgärden krävde tillstånd

av domstol, att enskild skulle underrättas och att Säkerhets- och integritetsskyddsnämnden skulle utöva tillsyn.

Den beskrivna regleringen i LEK framstod enligt regeringens mening inte som ändamålsenligt utformad och den ansågs inte heller i tillräcklig grad uppfylla de krav på rättssäkerhet och integritetsskydd som måste ställas på sådana integritetskänsliga åtgärder (prop. 2011/12:55 s. 66). Under förundersökningen är, enligt vad regeringen uttalade, syftet att utreda ett brott och i det inledande utredningsskedet att utröna vem eller vilka som skäligen kan misstänkas för brottet (prop. 2011/12:55 s. 68). Inhämtningen av uppgifter under en förundersökning riktas mot personer som misstänks vara delaktiga i brottet. Detta innebar, uttalade regeringen, att partsintresset borde vara styrande för vilka principer som skulle ligga till grund för regelsystemet och att integritetsaspekten under förundersökningen främst tog sikte på den övervakade personen som potentiell part. De principer som styrde inhämtningen borde därför, enligt regeringen, så långt det var möjligt anknyta till de rättssäkerhetsprinciper som gällde för den som är skäligen misstänkt. Inhämtning av uppgifter om elektronisk kommunikation i en förundersökning borde därför alltid äga rum inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation. Därigenom kom inhämtningen att omfattas av rättegångsbalkens bestämmelser om tillstånd av domstol till hemlig övervakning, underrättelse till enskild och användning av överskottsinformation. Enligt regeringens uppfattning var detta från rättssäkerhetssynpunkt av stort värde (prop. 2011/12:55 s. 68).

Mot den angivna bakgrunden upphävdes de aktuella bestämmelserna i LEK den 1 juli 2012. I förundersökningar kan uppgifter som angår särskilda elektroniska meddelanden därför inhämtas från leverantörerna enbart efter beslut om hemlig övervakning av elektronisk kommunikation. Skyldigheten för leverantörerna att lämna ut abonnemangsuppgifter i samband med misstanke om brott regleras dock även i fortsättningen i LEK, och är sedan den 1 juli 2012 inte begränsad till brott av viss svårhet (prop. 2011/12:55 s. 101–103).

Syftet med uppgiftsutlämnandet enligt artikel 17 är enbart att identifiera de tjänsteleverantörer som deltagit vid överföringen av ett meddelande så att uppgifter kan säkras även hos dem. Även om syftet är att utreda ett brott och att i förlängningen utröna vem eller vilka som skäligen kan misstänkas för brottet, skiljer sig inhämtning av uppgifter om vilka tjänsteleverantörer som deltagit vid över-

föringen av ett meddelande från inhämtning av uppgifter inom ramen för hemlig övervakning av elektronisk kommunikation på så sätt att den inte riktas mot personer som misstänks vara delaktiga i brottet. Den integritetsaspekt under en förundersökning, som främst tar sikte på den övervakade personen som potentiell part kommer in först i ett senare skede av förundersökningen i samband med att uppgifter (trafikuppgifter eller andra uppgifter) som exempelvis har säkrats genom ett bevarandeföreläggande ska lämnas ut.

Det uppgiftsutlämnande som nu avses inbegriper inte heller sådana aspekter av rätten till respekt för privat- och familjeliv, hem och korrespondens som avses i artikel 8 i Europakonventionen. Att de tjänsteleverantörer som deltagit vid överföringen av ett meddelande identifieras innebär inte något ingrepp i den privata sfär som artikeln är avsedd att skydda. Uppgifter om vilka tjänsteleverantörer som har medverkat utgör inte något intrång *i* enskildas korrespondens, utan innebär enbart att *sändningsvägarna* för korrespondensen (men alltså inte vem som korresponderade med vem) urskiljs. Vilken väg ett elektroniskt meddelande tar för att nå fram till adressaten från avsändaren är inte heller något som är direkt kopplad till den enskildes val, utan styrs tämligen slumpmässigt. Den enskilde råder alltså inte som huvudregel över om informationen överförs med hjälp av en eller flera tjänsteleverantörer.

Ett utlämnande av uppgifter som behövs för att kunna spåra ett meddelandes färdväg i syfte att identifiera vilka tjänsteleverantörer som har deltagit vid överföringen inbegriper således inte några egentliga integritetsaspekter. En begäran att få ut sådana uppgifter från en leverantör kan inte heller betraktas som ett straffprocessuellt tvångsmedel. Den naturliga platsen för en bestämmelse om utfående av uppgifter om ett meddelandes färdväg i det syfte som nu avses är, enligt vår mening, i LEK.

Mot bakgrund av det anförda är vårt förslag att leverantörerna enligt LEK ska vara skyldiga att till den myndighet som beslutat om ett bevarandeföreläggande lämna ut uppgift om vilka övriga leverantörer som har deltagit vid överföringen av det meddelande som omfattas av bevarandeföreläggandet. Bestämmelsen bör lämpligen tas in i 6 kap. 22 § LEK, som gäller undantag från den tystnadsplikt som gäller enligt 6 kap. 20 § första stycket LEK.

I första hand kommer uppgifterna att lämnas till åklagar- eller polismyndighet, men om bevarandeföreläggandet meddelats av Tullverket med stöd av 19 § smugglingslagen kan uppgifter lämnas ut även till Tullverket. Som nämnts i avsnitt 8.3.2 är det emellertid

vår uppfattning att Tullverket i ytterst få fall i praktiken kommer att besluta om bevarandeföreläggande. Det förhållandet utgör dock inte skäl att undanta andra myndigheter än åklagar- och polismyndighet från möjligheten att få ut uppgifter som behövs för att identifiera tjänsteleverantörerna, i de fall då annan myndighet än dessa faktiskt har beslutat om bevarandeföreläggande.

Det enda syftet är alltså att de brottsutredande myndigheterna ska få möjlighet att *identifiera* vilka *leverantörer* som deltagit vid överföringen, så att ett föreläggande om bevarande kan riktas även mot dessa. Det är således inte fråga om att ge de brottsutredande myndigheterna en möjlighet att kringgå reglerna om hemlig övervakning av elektronisk kommunikation och på ett lättare sätt få tillgång till trafikuppgifter som är avsedda att användas som bevis mot någon, t.ex. i fråga om vem som kommunicerade med vem vid en viss tidpunkt, på vilket sätt och hur länge. Enbart uppgift om vilka leverantörer som har deltagit vid överföringen ska lämnas ut. Som framgått är det vår uppfattning att ett utlämnande av dessa uppgifter inte innebär något nämnvärt intrång i enskildas integritet. Det ska alltså vara möjligt att få reda på från vilken leverantör som meddelandet sändes och – för det fall det har vidaresänts – till vilken leverantör det vidaresändes.

För att kunna lämna ut de uppgifter som avses måste den leverantör som får begäran ha fått del av eller tillgång till sådana uppgifter som avses i 6 kap. 20 § första stycket 3 LEK och som där anges som ”annan uppgift som angår ett särskilt elektroniskt meddelande”. För att förhindra att integritetskänslig information lämnas ut till den myndighet som begär att få uppgift om de leverantörer som deltagit i överföringskedjan och ur vilken exempelvis skulle kunna härledas vem som kommunicerade med vem, anser vi att den uppgift som ska lämnas ut är just uppgift om vilken eller vilka de övriga leverantörerna är. Några andra uppgifter ska alltså inte kunna gå att få ut med stöd av den nya bestämmelsen. För att tillgodose integritetsintresset och för att motverka att någon form av överskottsinformation lämnas ut, får det alltså ankomma på leverantören att ur den information som denne har tillgång till ta reda på vilka övriga leverantörer är. Av detta följer också att det inte finns någon information att lämna ut, om den leverantör mot vilken begäran riktas inte har uppgifter om vilka övriga leverantörer är. Vårt förslag innebär alltså inte något nytt krav på att spara uppgifter.

Med uppgift om vilka övriga leverantörer är avses uppgift om vilka övriga tillhandahållare av *elektroniska kommunikationsnät* eller *elektroniska kommunikationstjänster* som har deltagit vid överföringen av meddelandet. Genom att begränsa kretsen till dessa aktörer, men samtidigt inte ställa krav på att nätet eller tjänsten ska vara allmänt respektive allmän, uppfylls enligt vår mening konventionens krav på identifiering av tjänsteleverantörerna (jfr konventionens definition av tjänsteleverantör, avsnitt 5.2) samtidigt som det blir en möjlig och rimlig uppgift för den som begäran riktas mot att ta fram de efterfrågade uppgifterna.

Vår uppfattning är att uppgifter om vilka övriga leverantörer som deltagit vid överföringen av ett meddelande i den övervägande delen av fallen kommer att kunna fås fram genom de trafikuppgifter som lagras enligt 6 kap. 16 a § LEK. Leverantörerna kommer då, enligt 6 kap. 16 e § LEK, ha rätt till ersättning för kostnader som uppstår i samband med att uppgift om vilka övriga leverantörer är lämnas ut.

Enligt 6 kap. 16 c § LEK får uppgifter som omfattas av leverantörers lagringsskyldighet enligt 6 kap. 16 a § endast behandlas för att lämnas ut enligt vissa uppräknade bestämmelser. Eftersom sådana uppgifter om övriga leverantörer som en leverantör enligt vårt förslag ska vara skyldig att lämna ut, alltså kan bestå av vissa uppgifter som lagrats enligt 6 kap. 16 a § LEK, krävs ett tillägg i 6 kap. 16 c § LEK, så att uppgifter som lagrats även får behandlas för att lämnas ut enligt den föreslagna nya punkten i 6 kap. 22 §.

Enligt 6 kap. 21 § LEK har leverantörerna tystnadsplikt bl.a. för uppgift som hänför sig till användning av vissa hemliga tvångsmedel och för begäran om utlämnande av uppgift om abonnemang och som gäller misstanke om brott. Tystnadsplikt bör gälla även för begäran om utlämnande av uppgift om vilka övriga leverantörer som deltagit i överföringskedjan av ett meddelande som omfattas av ett bevarandeföreläggande.

8.3.4 En möjlighet till föreläggande att lämna upplysningar i syfte att underlätta husrannsakan i it-miljö införs

Förslag: Den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där ska kunna föreläggas att lämna de upplysningar som behövs för att ett beslut om husrannsakan ska

kunna verkställas. Beslut om föreläggande, som ska dokumenteras, får meddelas av undersökningsledaren eller åklagaren.

Om någon skäligen kan misstänkas för brottet får föreläggande inte riktas mot den misstänkte. Föreläggande får inte heller riktas mot den som, om åtal väcks, inte skulle vara skyldig att vittna i målet eller om sådan uppgift som de brottsutredande myndigheterna vill få tillgång till.

Vägrar den förelagde att lämna upplysningar får på undersökningsledarens eller åklagarens begäran vittnesförhör med honom eller henne äga rum inför rätten. Om förhöret gäller i tillämpliga delar vad som föreskrivs om bevisupptagning utom huvudförhandling. En misstänkt får beredas tillfälle att närvara vid förhöret om det kan ske utan men för utredningen.

Skälen för förslaget

Enligt artikel 19.4 ska det finnas en möjlighet i nationell rätt för 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 i systemet, att i den mån det är skäligt lämna den information som är nödvändig för att möjliggöra husrannsakan i it-miljö.

Vi har i avsnitt 5.4.7 gjort bedömningen att de svenska reglerna om vittnesförhör inför rätta visserligen formellt sett får anses uppfylla de krav som ställs upp i artikel 19.4, men att det finns skäl att överväga att i svensk rätt införa en specifik möjlighet till föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö.

Som vi tidigare redogjort för (se avsnitt 5.4.7) finns enligt polis och åklagare ett praktiskt behov av att införa en sådan möjlighet till föreläggande. Erfarenheten är att systemadministratörer och andra personer med kunskap om det datasystem som ska undersökas vid en husrannsakan inte alltid utan något författningsstöd vill samarbeta med de brottsutredande myndigheterna och att detta inte sällan innebär att husrannsakan blir resultatlös och att de uppgifter som myndigheten söker efter förstörs eller ändras innan de kan säkras. Det påtryckningsmedel som för närvarande står till buds – vittnesförhör inför rätta under förundersökningen – bedöms i dessa fall inte vara tillräckligt verkningsfullt i dess nuvarande form och används därför i praktiken aldrig. Vittnesförhör inför rätta under

förundersökningen förutsätter att någon är skäligen misstänkt, vilket inte behöver vara fallet i det skede av förundersökningen då husrannsakan vidtas. Förfarandet kräver vidare medverkan av rätten, varför det sällan kan användas så skyndsamt som krävs för att bevisningen ska undgå att förstöras. Eftersom den misstänkte även ska ges tillfälle att närvara vid förhöret finns det också en risk för att förundersökningen skadas.

Mot bakgrund av det anförda är det vår uppfattning att det bör införas en möjlighet till föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö. Det bör göras genom en särskild upplysningsplikt i förening med en effektivisering av förutsättningarna för vittnesförhör under en förundersökning.

Eftersom upplysningsplikt alltså ska kunna aktualiseras i samband med att ett beslut om husrannsakan verkställs är den naturliga placeringen av bestämmelsen i 28 kap. rättegångsbalken.

Vid utformningen av en bestämmelse om upplysningsplikt måste bl.a. tas ställning till vem som ska kunna åläggas upplysningsplikt, vad upplysningsplikten ska omfatta, vem som ska ha befogenhet att fatta beslut om upplysningsplikt och vilka sanktioner som ska finnas att tillgå för det fall upplysningsplikten inte följs.

Syftet är således att de brottsutredande myndigheterna inom ramen för en husrannsakan ska få tillgång till vissa upplysningar som behövs för att ge åtkomst till och kunna leta efter bevis i en dator eller ett datasystem. Föreläggande bör därför kunna riktas mot systemadministratörer eller andra personer som har kunskap om det datasystem som ska genomsökas. Vi föreslår mot den bakgrunden att föreläggande ska kunna riktas mot den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där. Det ska alltså finnas konkreta omständigheter av viss styrka som pekar på att den person som föreläggs känner till det datasystem som de brottsutredande myndigheterna vill genomsöka. I begreppet ”datasystem” innefattas datorer, program, servrar m.m. liksom den tekniska lösningen och utformningen (jfr Svenska datatermgruppens ordlista, ordlisteartikel 64).

Föreläggandet bör innebära att den förelagda personen ska lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Vilka upplysningar som behövs är beroende av omständigheterna i det enskilda fallet. Det kan röra sig om att beskriva datasystemet, uppge lösenord och åtkomstkoder, lämna

dekrypteringsnycklar eller att ange vilken av ett flertal servrar som den information som de brottsutredande myndigheterna vill genomsöka finns lagrad på.

Ett föreläggande att lämna upplysningar inom ramen för en husrannsakan bör kunna ges skyndsamt i samband med att husrannsakan verkställs. Något krav på att någon är skäligen misstänkt kan mot den bakgrunden inte uppställas. Om utredningen emellertid har kommit så långt att det finns en skäligen misstänkt för det brott som utreds ska den misstänkte inte vara tvingad att ge polis och åklagare tillgång till information och bevis som kan användas mot honom eller henne. Föreläggande ska därför inte kunna riktas mot någon som är misstänkt för brottet.

Även vissa andra personer bör undantas från upplysningsplikten. Enligt vår uppfattning är en lämplig avgränsning av denna personkrets reglerna om vittnesplikt. Om man från upplysningsplikten undantar den som, om åtal hade väckts, inte skulle vara skyldig att vittna i målet och att därvid lämna sådana uppgifter som avses omfattas av föreläggandet, dvs. upplysningar om åtkomstkod, lösenord etc., kommer föreläggande att lämna upplysningar exempelvis inte att kunna riktas mot den misstänktes närstående eller mot hans eller hennes försvarare, om denne exempelvis har fått del av sin klients lösenord vid fullgörande av sitt uppdrag.

Ett föreläggande att lämna upplysningar kommer med en hänvisning till reglerna om vittnesplikt inte heller att kunna riktas mot en målsägande. Enligt vår uppfattning är det rimligt att en målsägande inte mot sin vilja tvingas att medverka. Som nämnts i avsnitt 5.4.7 är inte heller avsikten enligt artikel 19.4 att föreläggande att lämna information ska riktas mot målsägande. De praktiska problemen med att få målsägande att medverka i nu avsedda fall är enligt vår uppfattning även små.

Eftersom föreläggande att lämna upplysningar ska kunna utfärdas skyndsamt i samband med att ett beslut om husrannsakan verkställs, bör ett beslut om att ge föreläggande kunna fattas av personer som finns på platsen där husrannsakan genomförs, eller av personer som dessa enkelt kan ta kontakt med. Enligt vår uppfattning bör föreläggande inte kunna beslutas av enskild polisman, utan enbart av undersökningsledaren eller åklagaren. Det finns inte anledning att låta rätten besluta om föreläggande. Även i det fall beslutet om husrannsakan fattats av rätten enligt 28 kap. 4 § första stycket rättegångsbalken, på grund av att husrannsakan kunde antas bli av stor omfattning eller medföra synnerlig olägenhet för den

hos vilken åtgärden skulle vidtas, bör således föreläggande att lämna upplysningar beslutas av undersökningsledaren eller åklagaren. I de fall då förundersökningen leds av Tullverket med stöd av 19 § smugglingslagen kommer föreläggande att lämna upplysningar även att kunna ges av den befattningshavare vid Tullverket som leder förundersökningen och som beslutat om husrannsakan (se 19 § smugglingslagen och den hänvisning som där finns till rättegångsbalkens bestämmelser).

Eftersom föreläggandet ska kunna meddelas skyndsamt i samband med att en husrannsakan verkställs bör det inte krävas att föreläggandet ges i skriftlig form. Enligt vår uppfattning är det tillräckligt att beslutet om föreläggande dokumenteras.

Mot den som förelagts att lämna upplysningar men vägrar att göra detta, bör finnas sanktioner. Enligt vår uppfattning är den lämpligaste sanktionen mot den som vägrar att bistå med upplysningar att undersökningsledaren eller åklagaren får begära att vittnesförhör med honom eller henne ska äga rum inför rätten. Om förhöret bör då i tillämpliga delar gälla vad som föreskrivs om bevisupptagning utom huvudförhandling. För det fall den förelagde även inför rätten skulle vägra att lämna upplysningar kan rätten, med stöd av 36 kap. 21 § rättegångsbalken, förelägga honom eller henne vid vite, och om det inte skulle vara verksamt, vid äventyr av häkte att lämna upplysningarna.

Till skillnad från vad som gäller enligt bestämmelserna i 23 kap. 13 § rättegångsbalken om vittnesförhör inför rätta under en förundersökning bör alltså inte krävas att någon skäligen kan misstänkas för brottet och även om det finns en skäligen misstänkt bör han eller hon få ges tillfälle att närvara vid förhöret endast om det kan ske utan men för utredningen.

Begränsningen i 23 kap. 13 § rättegångsbalken om att vittnesförhör vid rätten under förundersökningen inte får äga rum innan förundersökningen kommit så långt att någon skäligen kan misstänkas för brottet, tillkom under riksdagsbehandlingen. Motivet för begränsningsregeln är dels att det annars hade kunnat finnas en risk för att förhöret skulle ledas i viss riktning och att vittnena skulle kunna komma att lämna riktade berättelser som de sedan vid en huvudförhandling, av rädsla för att bli dömda för mened, inte skulle våga ändra, dels att det hade kunna ifrågasättas om inte vittnesförhör skulle kunna komma att begäras med den som misstänktes för brottet (Fitger, *Rättegångsbalken*, Del 2, 23:51). Även

bestämmelsen om att den misstänkte ska ha tillfälle att närvara vid förhöret tillkom under riksdagsbehandlingen.

Motivet för begränsningsregeln enligt 23 kap. 13 § rättegångsbalken som går ut på att de som hörs skulle kunna komma att lämna riktade berättelser som de sedan inte vågar rätta, har enligt vår mening ingen bärighet på den upplysningsplikt vid husrannsakan i it-miljö som nu föreslås. Upplysningsplikten, där förhör inför rätta alltså föreslås få användas som påtryckningsmedel, går enbart ut på att lämna viss konkret information så att en beslutad husrannsakan ska kunna verkställas. De uppgifter som ska lämnas är alltså inte uppgifter som primärt ska användas som bevis mot en misstänkt utan uppgifterna ska *leda till* uppgifter som sedan kan användas som bevis.

Skälet för begränsningsregeln som handlar om att det finns en risk för att det annars kan komma att begäras vittnesförhör med den som misstänks för brott har emellertid en viss relevans även för den upplysningsplikt som nu föreslås. Enligt vårt förslag får föreläggande om att lämna upplysningar emellertid inte riktas mot någon som skäligen kan misstänkas för brottet och inte heller mot någon av de personer som räknas upp i 36 kap. 1 § andra–fjärde styckena rättegångsbalken. Om krav på att någon ska vara skäligen misstänkt för brottet skulle ställas upp för att föreläggande ska få utfärdas, hade föreläggande helt enkelt inte kunnat användas i det tidiga skede av förundersökningen då det behövs. Även i detta sammanhang bör framhållas att det enbart handlar om att förmå någon som inte är misstänkt för det brott som utreds, att lämna ut vissa upplysningar vid en husrannsakan så att denna kan verkställas.

En upplysningsplikt som åläggs någon som polis och åklagare inte har någon avsikt att senare åtala står, enligt vår uppfattning, inte i strid med artikel 6 i Europakonventionen och rätten att inte belasta sig själv (förbudet mot *self-incrimination*). Principen innebär primärt att den som *är misstänkt* för brott inte ska behöva bidra till utredningen eller bevisningen i målet genom att göra medgivanden eller bistå med material som är belastande för honom eller henne (Danelius, *Mänskliga rättigheter i Europeisk praxis*, tredje upplagan, s. 247–248).

Enligt vårt förslag kan föreläggande att lämna upplysningar enbart riktas mot den som, om åtal väcks, skulle vara skyldig att vittna i saken om sådan uppgift som de brottsutredande myndigheterna vill få tillgång till genom föreläggandet. Enligt 36 kap. 6 § rättegångsbalken får ett vittne bl.a. vägra att yttra sig om en

omständighet, vars yppande skulle röja att vittnet eller någon vittnet närstående har gjort sig skyldig till brottslig eller vanärande handling. En person mot vilken ett föreläggande att lämna upplysningar riktas mot kan mot den bakgrunden inte tvingas att lämna upplysningar som senare kan komma att användas mot honom eller henne i ett brottmål. Den föreslagna bestämmelsen om föreläggande att lämna upplysningar kommer således inte i konflikt med rätten att inte belasta sig själv.

8.3.5 Bör möjligheten till förbehåll utnyttjas när det gäller insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter?

Förslag: Sverige ska avge förbehåll av innehåll att åtgärderna i artikel 20 endast tillämpas på sådana brott avseende vilka hemlig övervakning av elektronisk kommunikation kan användas. Förbehåll ska vidare avges av innehåll att åtgärderna i artikel 20 och 21 inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt.

Skälen för förslaget

Artiklarna 20 och 21 i konventionen innehåller bestämmelser om insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter.

Vi har i avsnitt 5.4.8 och 5.4.9 gjort bedömningen att svensk rätt genom bestämmelserna om hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation uppfyller kraven i konventionsartiklarna, om förbehåll av visst slag avges.

Såvitt avser artikel 20 om insamling i realtid av trafikuppgifter, har vi gjort bedömningen att svensk rätt uppfyller konventionskraven om förbehåll avges av innehåll att åtgärderna i artikeln dels endast tillämpas på sådana brott avseende vilka hemlig övervakning av elektronisk kommunikation kan användas, dels inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt.

När det gäller artikel 21 om avlyssning av innehållsuppgifter, har vi gjort bedömningen att svensk rätt uppfyller konventionskraven om förbehåll avges av innehåll att åtgärderna i artikeln inte tillämpas på meddelanden som endast överförs i ett elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt.

Vi föreslår därför att möjligheten till förbehåll enligt artikel 14.3 a utnyttjas såvitt avser artikel 20 och att möjligheten till förbehåll enligt artikel 14.3 b utnyttjas såvitt avser såväl artikel 20 som 21.

8.4 Anpassningen av regleringen om internationell rättslig hjälp

8.4.1 Utgångspunkter

Vi har i avsnitt 5.6 gjort bedömningen att svensk rätt till stor del redan uppfyller de krav som konventionen ställer i fråga om internationellt samarbete, men att lagstiftningsåtgärder krävs såvitt avser rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och skyndsamt röjande av vissa trafikuppgifter (artikel 29 respektive 30).

I avsnitt 6.5 har vi gjort bedömningen att det inte krävs några ytterligare lagändringar för att tillgodose de krav som följer av tilläggsprotokollet i fråga om regler om internationellt samarbete än de som följer av konventionens bestämmelser.

De ändringar som är aktuella är att hänföra till lagen (2000:562) om internationell rättslig hjälp i brottmål (Lirb).

När Lirb infördes gavs den ett vidare tillämpningsområde än vad som krävdes med hänsyn till då gällande internationella åtaganden. Syftet var att för framtiden skapa utrymme för ett utvidgat internationellt samarbete. Utgångspunkten för regleringen är att alla åtgärder som är möjliga att vidta i en svensk förundersökning också ska vara tillgängliga för en annan stat efter en ansökan om rättslig hjälp, oavsett om bistånd med åtgärden föreskrivs i en internationell överenskommelse eller inte. Enligt våra direktiv måste eventuella förslag till ändringar i lagen med anledning av tillträdet till konventionen vara anpassade till denna grundläggande systematik i regleringen. Vi måste också beakta redan ingångna internationella åtaganden som kan beröras av ändringsförslagen.

I det följande redovisas våra förslag till lagstiftning för att tillgodose konventionens krav på rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter och överväganden i fråga om behovet av ytterligare lagändringar än de som föreslagits i avsnitt 8.3.3 när det gäller rättslig hjälp med skyndsamt röjande av vissa trafikuppgifter.

8.4.2 En möjlighet till rättslig hjälp med skyndsamt bevarande av lagrade uppgifter i elektronisk form införs

Förslag: Möjligheten att förelägga någon som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften, räknas upp som en av de åtgärder som omfattas av rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål.

Rättslig hjälp med bevarandeföreläggande ska få lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag.

En ansökan om bevarandeföreläggande ska handläggas av åklagare. Av ansökan ska framgå sådana uppgifter som behövs för att åtgärden ska kunna genomföras.

Åklagaren ska genast pröva om det finns förutsättningar för åtgärden. Om bevarandeföreläggande beslutas ska detta gälla för en period om minst 60 dagar.

Sverige ska förbehålla sig rätten att avslå en framställning om säkrande av lagrade datorbehandlingsbara uppgifter, om det finns skäl att tro att villkor om dubbel straffbarhet inte kan uppfyllas när uppgifterna ska röjas.

Bedömning: Några ytterligare lagstiftningsåtgärder än de som föreslagits som ett led i anpassningen till kraven på skyndsamt partiellt röjande av trafikuppgifter i nationellt förfarande krävs inte för att uppfylla kraven på rättslig hjälp med skyndsamt röjande av vissa trafikuppgifter.

Skälen för förslaget och bedömningen

Artikel 29 i konventionen behandlar rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter, dvs. rättslig hjälp med sådant säkrande som avses i artikel 16.

Vi har i avsnitt 5.6.8 gjort bedömningen att det krävs lagstiftning för att uppfylla konventionskravet enligt artikel 29 eftersom det i en svensk förundersökning inte är möjligt att få till stånd ett sådant skyndsamt säkrande som avses i artikel 16 och det då inte heller är möjligt att ge en annan stat rättslig hjälp med åtgärden.

I avsnitt 8.3.2 har vi lämnat förslag till lagstiftning som behövs för att uppfylla kraven i artikel 16. Om det bevarandeföreläggande som föreslås i avsnittet är möjligt att utfärda även på ansökan av en annan stat uppfyller svensk rätt även de krav som ställs upp i artikel 29. Vi föreslår därför att åtgärden räknas upp som en av de åtgärder som omfattas av rättslig hjälp enligt Lirb.

Som tidigare nämnts har Lirb ett vidare tillämpningsområde än vad som krävs med hänsyn till gällande internationella åtaganden och utgångspunkten för regleringen är att alla åtgärder som är möjliga att vidta i en svensk förundersökning också ska vara tillgängliga för en annan stat efter en ansökan om rättslig hjälp, oavsett om bistånd med åtgärden föreskrivs i en internationell överenskommelse eller inte. För att de nya reglerna om rättslig hjälp med skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter ska harmoniera med denna grundläggande systematik i regleringen är det vår uppfattning att reglerna ska vara generellt tillämpliga, och inte enbart kunna användas när den ansökande staten har tillträtt konventionen.

Av artikel 29.3 framgår att villkor om dubbel straffbarhet inte ska ställas upp för sådant säkrande som avses i artikel. Enligt artikel 29.4 får samtidigt en stat som ställer upp dubbel straffbarhet som villkor för att besvara en framställning om rättslig hjälp med åtkomst till och röjande av uppgifter, när det gäller andra brott än de som upptas i konventionen, förbehålla sig rätten att avslå en framställning om säkrande om den har skäl att tro att villkoret om dubbel straffbarhet inte kan uppfyllas när uppgifterna ska röjas.

Vi har i avsnitt 8.3.2 anfört att det bevarandeföreläggande som föreslås endast syftar till att under en begränsad tidsperiod säkra elektroniska uppgifter som redan finns lagrade, och att det är först när uppgifterna ska lämnas ut som integritetsaspekter gör sig gällande. Mot den bakgrunden är det vår uppfattning att det inte är

nödvändigt att ställa upp krav på dubbel straffbarhet för att ge rättslig hjälp med åtgärden. Att krav på dubbel straffbarhet inte uppställs innebär också en lättnad vid prövningen av om rättslig hjälp med åtgärden kan beviljas. Detta är en förutsättning för att ett säkrande av uppgifter kan göras så skyndsamt som konventionen förutsätter.

Vi föreslår inte någon ändring i de regler som gäller för rättslig hjälp med åtkomst till uppgifter som bevarats. För åtkomst till uppgifterna ska således även i fortsättningen tillämpas de regler i Lirb som gäller för bl.a. beslag, hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation. För hjälp med dessa åtgärder ställs som huvudregel upp krav på dubbel straffbarhet. I avsnitt 8.3.2 har vi fäst uppmärksamhet på att proportionalitetsprincipen generellt gäller vid beslut om och användning av tvångsmedel och att denna kommer att gälla även när det gäller föreläggande att bevara elektroniska uppgifter. Som anförts i avsnittet innebär proportionalitetsprincipen att de brottsbekämpande myndigheterna inte ska meddela ett bevarandeföreläggande om de redan då de överväger att meddela föreläggandet kan se att det, mot bakgrund av brottets svårhet eller av andra skäl, inte finns någon möjlighet att med stöd av de regler som gäller för detta, senare få ut de uppgifter som skulle säkras. Motsvarande bör vara fallet om det redan då uppgifterna ska säkras kan förutspås att uppgifterna, mot bakgrund av krav på dubbel straffbarhet, inte kommer att kunna lämnas ut. För att ge utrymme att vägra rättslig hjälp med säkrande av uppgifter i den angivna situationen bör möjligheten till förbehåll enligt artikel 29.4 utnyttjas.

En ansökan om skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter, dvs. en ansökan om bevarandeföreläggande, bör handläggas av åklagare. Av ansökan bör, utöver vad som generellt anges i 2 kap. 4 § Lirb, framgå sådana uppgifter som behövs för att åtgärden ska kunna genomföras, dvs. bl.a. uppgifter om vilka lagrade uppgifter som ska säkras och var och hos vem uppgifterna finns (jfr artikel 29.2). När en ansökan om säkrande kommit in bör åklagaren genast pröva om det finns förutsättningar för åtgärden. Om bevarandeföreläggande beslutas, bör detta gälla för en period om minst 60 dagar, så att den ansökande staten får tid på sig att förbereda en ansökan om åtkomst till uppgifterna (jfr artikel 29.7). Samtidigt gäller den generella regeln att förordnandet inte får gälla längre än 90 dagar, med möjlighet till 30 dagars förlängning om det finns särskilda skäl.

Enligt artikel 29.6 ska den anmodade staten om den bl.a. anser att ett säkrande inte kommer att trygga den framtida tillgängligheten till uppgifterna eller på något sätt kommer att störa den ansökande statens brottsutredning genast underrätta den ansökande staten om detta, som då får avgöra om framställningen ändå ska verkställas. I 2 kap. 8 § Lirb finns redan bestämmelser om i vilka situationer den åklagare eller tingsrätt som handlägger ett ärende om rättslig hjälp ska underrätta den utländska myndigheten eller staten om handläggningen. Av bestämmelsens tredje stycke följer exempelvis att en åklagare omedelbart ska underrätta den ansökande staten om det under handläggningen av ett ärende om rättslig hjälp kommer fram att det kan vara lämpligt att vidta även en annan åtgärd än den som begärts. Så skulle kunna vara fallet om åklagaren är av uppfattningen att det finns risk för att de uppgifter som ska säkras går förlorade trots att ett bevarandeföreläggande meddelas och att det i stället är lämpligare att tillämpa regler om beslag.

Av artikel 30 i konventionen följer att en stat, som vid verkställandet av en framställning om skyndsamt säkrande av trafikuppgifter enligt artikel 29 upptäcker att en tjänsteleverantör i en annan stat har medverkat i överföringen av meddelandet, snabbt för den ansökande staten ska röja den mängd trafikuppgifter som behövs för att identifiera tjänsteleverantören och den väg på vilken meddelandet överfördes. Vi har i avsnitt 5.6.9 gjort bedömningen att det krävs lagstiftning för att uppfylla konventionens krav i denna del, eftersom sådant skyndsamt röjande inte går att få till stånd inom ramen för en nationell förundersökning och det då inte heller går att ge rättslig hjälp med detta.

Vi har i avsnitt 8.3.3, i syfte att uppfylla kraven i artikel 17 på skyndsamt röjande av uppgifter i ett nationellt säkrandeförfarande, föreslagit att det i LEK införs en skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst att lämna ut uppgift om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande till den myndighet som meddelat föreläggandet.

Att med stöd av en leverantörs skyldighet enligt LEK hämta in uppgifter om vilka övriga leverantörer som har deltagit vid överföringen av ett meddelande är enligt vår uppfattning, till skillnad från utfärdande av ett bevarandeföreläggande, inte något straffprocessuellt tvångsmedel eller någon tvångsåtgärd. Enligt 1 kap. 2 §

andra stycket Lirb hindrar lagen inte att hjälp lämnas med annan åtgärd än sådan som räknas upp i lagen om det kan ske utan tvångsmedel eller annan tvångsåtgärd. Om vår föreslagna reglering i LEK genomförs, kommer således sådana uppgifter som avses i artikel 30 kunna överlämnas till en annan stat med stöd av regleringen i 1 kap. 2 § andra stycket Lirb. Något krav på dubbel straffbarhet finns inte för sådant överlämnande. Några ytterligare lagstiftningsåtgärder än de som föreslagits som ett led i anpassningen till artikel 17 krävs därför inte för att uppfylla kraven i artikel 30.

9 Straffskalorna för brytande av post- eller telehemlighet och dataintrång

9.1 Inledning

I vårt uppdrag ingår att analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF (direktivet). Vi har i avsnitt 7 redovisat vilket behov av lagändringar som direktivet föranleder. Artikel 9 i direktivet innehåller specifika bestämmelser om straffskalornas utformning när det gäller olika former av angrepp mot informationssystem. I avsnitt 7.3.7 har vi gjort bedömningen att det krävs lagstiftning för att uppfylla artikelns krav på att samtliga sådana straffbara befattningar med verktyg som avses i artikel 7 ska vara belagda med ett maximistraff på minst två års fängelse, eftersom straffskalan för förberedelse till dataintrång inte ens teoretiskt går längre än till fängelse 1 år och 364 dagar. Vi har vidare gjort bedömningen att det krävs lagstiftning för att uppfylla artikelns krav på att brotten olaglig systemstörning och olaglig datastörning i de fall som avses i artikel 9.3 och 9.4 ska vara belagda med ett maximistraff på minst tre respektive fem års fängelse. Brotten olaglig systemstörning och olaglig datastörning motsvaras i svensk rätt främst av brottet dataintrång. Det finns således redan mot bakgrund av direktivet anledning att överväga att skärpa straffskalan för dataintrång.

Brotten brytande av post- eller telehemlighet och dataintrång har straffskalor som sträcker sig från böter till fängelse i högst två år. Straffskalan för brytande av post- eller telehemlighet har varit oförändrad sedan brottsbalkens tillkomst. Även dataintrångsbestämmelsen har samma straffskala som när bestämmelsen först infördes

i datalagen (1973:289), även om den ändrats i sak vid ett flertal tillfällen.

Som framhålls i våra direktiv har det sedan brottsbalkens och datalagens tillkomst skett en betydande samhällsutveckling och elektroniska informationssystem har i dag en ojämförligt större betydelse i samhället än när bestämmelserna infördes. Enligt direktiven finns tecken på att utvecklingen går mot allt farligare och mer storskaliga angrepp mot informationssystem, till exempel intrång i eller överbelastningsattacker mot bankers och myndigheters informationssystem. Angreppen begås, enligt direktiven, med sofistikerade metoder och kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och kommunikation och kan också leda till förlust eller förvanskning av hemlig eller i övrigt särskilt integritetskänslig information. Många gånger kan ett sådant beteende träffas av straffansvaret för sabotage i 13 kap. 4 § brottsbalken. Beroende på omständigheterna, t.ex. att skadan i och för sig är omfattande men av tillfällig karaktär eller att den infrastruktur som skadas inte utgör för samhället viktig egendom, kan emellertid, framhålls i direktiven, vissa mycket straffvärda beteenden falla utanför sabotagebestämmelsens tillämpningsområde.

Mot den bakgrunden ingår det även i vårt uppdrag att, vid sidan av vad som bedöms nödvändigt för att genomföra EU-direktivet, överväga behovet av och – om det finns anledning till det – lämna förslag till skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem. Vi ska i det sammanhanget redovisa vår bedömning av om en sådan straffskärpning bör ske enbart genom förändringar av straffskalorna eller om särskilda straffskalor för grova brott bör införas. De straffrättsliga och systematiska konsekvenserna av dessa alternativ ska då beskrivas.

9.2 Kriminalstatistik

9.2.1 Allmänt om de statistiska uppgifterna

Brottsförebyggande rådet (Brå) ansvarar för och publicerar den officiella kriminalstatistiken. I den beskrivs bl.a. den brottslighet som kommer till myndigheternas kännedom genom polisanmälningar.

Brott som inte anmäls och som inte observeras kommer inte med i kriminalstatistiken.

Den officiella kriminalstatistiken omfattar brottsstatistik, statistik över för brott lagförda personer, kriminalvårdsstatistik och statistik över återfall i brott. Den årliga sammanställningen av brottsstatistiken innehåller uppgifter om anmälda brott, uppklarade brott och personer misstänkta för brott. Statistiken över för brott lagförda personer benämns vanligen lagföringsstatistik (*Konsten att läsa statistik om brottslighet*, Brå-rapport 2006:1 s. 11).

I detta avsnitt redogörs för kriminalstatistiken beträffande brottet dataintrång avseende anmälda brott, uppklarade brott, lagföringsbeslut och påföljdsval. Redovisningen bygger uteslutande på statistik och analysmaterial från Brå. När det gäller brottet brytande av post- eller telehemlighet redovisas det inte särskilt i Brå:s brottsstatistik utan i en samlingskategori som även omfattar bl.a. olaga tvång och olovlig avlyssning. Någon brottsstatistik avseende brytande av post- eller telehemlighet finns därför inte i avsnittet. Avsnittet innehåller emellertid statistiska uppgifter om lagföring och påföljdsval avseende brytande av post- eller telehemlighet.

För att tolka uppgifterna i kriminalstatistiken krävs kunskap om vad uppgifterna avser och hur statistiken är uppbyggd. Statistiken över anmälda brott omfattar händelser som anmälts eller av myndighet observerats som brott och blivit registrerade av polis, tull eller åklagare. Statistiken över uppklarade brott omfattar händelser som anmälts som brott och sedan fått ett beslut som gör att brottet räknas som uppklarat. Lagföringsstatistiken däremot utgår från den eller de personer som begått brottet eller brotten och omfattar alla lagförda personer under ett år. Om en person har lagförts flera gånger under ett år förekommer personen flera gånger i statistiken. De två statistikområdena brottsstatistik (bl.a. anmälda och uppklarade brott) och lagföringsstatistik redovisar alltså helt olika typer av enheter, vilket gör att det är svårt att jämföra antalet lagförda personer med antalet brott. Lagföringsstatistiken redovisar också i de flesta fall endast det s.k. huvudbrottet i lagföringen, medan statistiken över anmälda och uppklarade brott redovisar samtliga brott som registrerats som brott. Analysen kompliceras av att gärningar efter anmälningstillfället kan komma att omrubriceras, omklassificeras eller bedömas inte vara ett brott utan att anmälningsstatistiken ändras. Ett brott som anmäls ett år kan också komma att klaras upp eller leda till lagföring först under senare år (Brå-rapport 2006:1 s. 28–29 och 58–59).

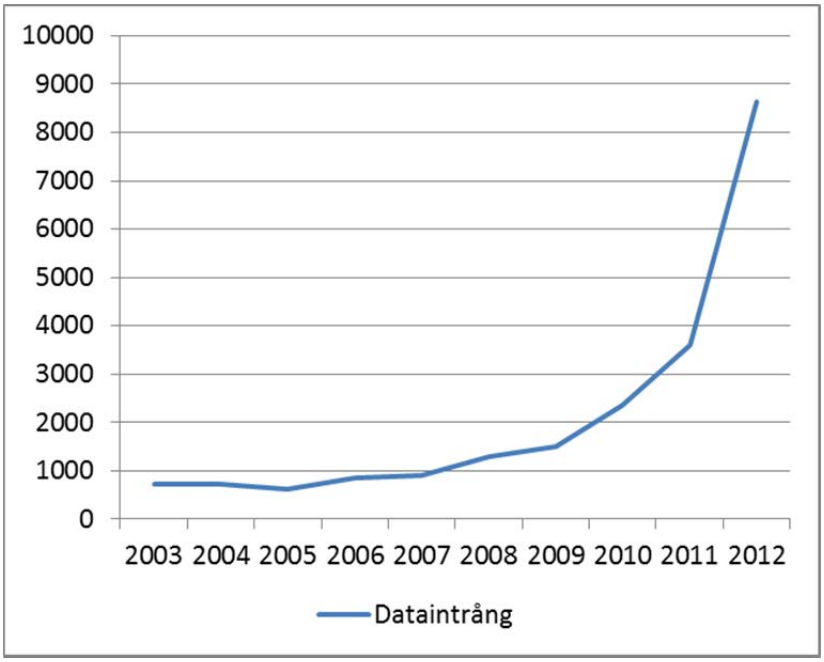
9.2.2 Polisanmälda dataintrång

Antalet polisanmälda dataintrång uppgick år 2012 till 8 646 enligt den officiella kriminalstatistiken. Sedan år 2003 har antalet anmälda brott avseende dataintrång ökat från 731 år 2003 till 8 646 år 2012. Antalet anmälda dataintrång har alltså ökat med nästan 1 100 procent under denna tioårsperiod.

Av diagrammet nedan framgår att antalet anmälda dataintrång ökat i princip årligen sedan 2003. Den senaste tvåårsperioden har antalet anmälda brott mer än fördubblats: från 3 597 år 2011 till 8 646 år 2012.

Statistiken över antal anmälda brott utgår från anmälningstillfället och speglar således polisens kategorisering av anmälarens berättelse.

Diagram **Antal anmälda dataintrång åren 2003–2012**



Källa: Brå

9.2.3 Uppklarade dataintrång

I statistiken över uppklarade brott redovisas de anmälda brott som åtgärdats under ett kalenderår. Begreppet ”uppklarade brott” innebär dock endast att brottet fått ett ”polisiärt klarläggande”, och behöver inte betyda att man har bundit en gärningsman till brottet (Brå-rapport 2006:1 s. 32). De uppklarade brotten delas i statistiken upp i kategorierna personuppklarade brott, där åklagaren ansett sig kunna knyta en gärningsman till brottet, och tekniskt uppklarade brott, där utredningen av brottet lags ned av olika skäl. Om ett brott är *personuppklarat* har beslut om att väcka åtal, utfärda strafföreläggande eller meddela åtalsunderlåtelse fattats. De vanligaste besluten som innebär att brott i statistiken redovisas som *tekniskt uppklarade* avser att det inte kan styrkas att ett brott har begåtts, att den anmälda gärningen inte bedöms vara brott eller att den misstänkte inte är straffmyndig. De vanligaste besluten som innebär att brott anses som *ouppklarade* är att polis eller åklagare beslutat att spaningsuppslag saknas, att spaningarna inte lett till något resultat, att det trots utredning inte kan styrkas att den som varit skäligen misstänkt har begått brottet eller att utredningen visar att den skäligen misstänkte är oskyldig. De ouppklarade brotten redovisas inte i statistiken (Brå-rapport 2006:1 s. 32).

Uppklarningsprocenten redovisas i statistiken utifrån antalet brott som klarats upp ett visst år jämfört med antalet brott som anmälts samma år. Det kan, men behöver inte, finnas en direkt koppling mellan antalet anmälda brott och antalet uppklarade brott under ett och samma år. Medan de anmälda brotten endast hänför sig till det aktuella året kan ett brott som klarats upp samma år härröra från en anmälan flera år tillbaka i tiden.

Antalet dataintrång som klaras upp ett år i förhållande till antalet anmälda brott varierar till viss del men ligger i genomsnitt runt 50 procent. Under åren 2003–2012 varierade uppklarningsprocenten för dataintrång mellan lägst 31 procent (år 2003) och högst 78 procent (år 2004). Andelen personuppklarade dataintrång är låg. För dataintrång varierade andelen personuppklarade brott mellan 3–12 procent under åren 2003–2012. Den genomsnittliga personuppklarningsprocenten under perioden låg på drygt 6 procent.

9.2.4 Lagförda dataintrång och brytande av post- eller telehemlighet

Med lagföring avses i den officiella statistiken domslut (dom i tingsrätt), strafföreläggande eller åtalsunderlåtelse. En enskild person kan lagföras vid flera tillfällen under ett år. I statistiken redovisas en lagförd person för varje enskilt lagföringsbeslut som denne står för under perioden. Detta betyder att om flera personer ingår i samma lagföring redovisas varje person som en enhet för sig i statistiken. En person kan lagföras för flera brott i ett och samma lagföringsbeslut. Det förhållandet att lagföringsstatistiken avser domar i tingsrätt innebär att en person som befunnits skyldig i tingsrätt, men frikänts i högre instans, kommer att stå kvar som ”dömd” i statistiken. Eftersom frikännande domar inte redovisas kommer vidare en person som frikänts i tingsrätt men därefter fällts i högre instans inte att finnas med i lagföringsstatistiken. Lagföringsstatistiken avseende huvudbrott och huvudpåföljd redovisar brottet med den strängaste straffskalan. Av statistiken framgår inte om lagföringsbesluten avser ett eller flera brott (Brå-rapport 2006:1 s. 40–41).

Av *tabell 1* nedan framgår att antalet lagföringsbeslut för dataintrång i princip ökade konstant mellan åren 2002–2011[1] samt att ungefär hälften av lagföringarna består av domar. Övriga består således av strafföreläggande och åtalsunderlåtelser.

Av *tabell 2* nedan framgår att antalet lagföringar för brytande av post- eller telehemlighet är ytterst få, totalt 18 under hela den redovisade tioårsperioden, och att ungefär hälften av dem består av domar.

[1] Slutlig statistik över personer lagförda för brott 2012 kommer enligt Brå att finnas tillgänglig från den 30 maj 2013. De statistiska uppgifterna i avsnittet avser därför tioårsperioden 2002–2011.

Tabell 1 **Antal lagföringsbeslut efter dataintrång som huvudbrott, år 2002–2011**

År	Lagföringar totalt	Domslut
2002	20	12
2003	25	10
2004	33	16
2005	23	17
2006	25	10
2007	34	14
2008	36	18
2009	43	24
2010	53	33
2011	64	33

Källa: Brå

Tabell 2 **Antal lagföringsbeslut efter brytande av post- eller telehemlighet som huvudbrott, år 2002–2011**

År	Lagföringar totalt	Domslut
2002	1	1
2003	2	1
2004	2	1
2005	-	-
2006	1	-
2007	3	2
2008	2	-
2009	2	1
2010	3	1
2011	2	1

Källa: Brå

9.2.5 Påföljdsval för dataintrång och brytande av post- eller telehemlighet som huvudbrott

Den officiella kriminalstatistiken visar att böter är den vanligaste påföljden för såväl dataintrång som brytande av post- eller telehemlighet. Inte i något fall under åren 2002–2011[2] har fängelse

[2] Slutlig statistik över personer lagförda för brott 2012 kommer enligt Brå att finnas tillgänglig från den 30 maj 2013. De statistiska uppgifterna i avsnittet avser därför tioårsperioden 2002–2011.

bestämts som påföljd när huvudbrottet varit dataintrång eller brytande av post- eller telehemlighet. I endast två fall har en frivårdspåföljd i kombination med samhällstjänst dömts ut (år 2011 när huvudbrottet var dataintrång).

Av tabellerna nedan framgår vilken huvudpåföljd som dömts ut när huvudbrottet varit dataintrång (*tabell 3*) respektive brytande av post- eller telehemlighet (*tabell 4*). Kategorin ”annat” innefattar förutom andra påföljder än de särskilt redovisade även de fall då åtalsunderlåtelse bestämts.

Tabell 3 Val av påföljd för dataintrång som huvudbrott, åren 2002–2011

År	Lagföringar totalt	Fängelse	St/Vd (shtj)[3]	Böter	Annat[4]
2002	20	-	2	17	1
2003	25	-	1	19	5
2004	33	-	1	29	3
2005	23	-	3	19	1
2006	25	-	1	18	6
2007	34	-	2	26	6
2008	36	-	4	29	3
2009	43	-	9	30	4
2010	53	-	6	43	4
2011	64	-	10 (2)	44	10

Källa: Brå

[3] Skyddstillsyn/Villkorlig dom (i förekommande fall i kombination med samhällstjänst).
[4] Andra påföljder än de särskilt redovisade och åtalsunderlåtelse.

Tabell 4 Val av påföljd för brytande av post- eller telehemlighet som huvudbrott, åren 2002–2011

År	Lagföringar totalt	Fängelse	St/Vd (shtj)[5]	Böter	Annat[6]
2002	1	-	-	1	-
2003	2	-	-	1	1
2004	2	-	-	2	-
2005	-	-	-	-	-
2006	1	-	-	1	-
2007	3	-	1	1	1
2008	2	-	-	-	2
2009	2	-	1	-	1
2010	3	-	-	1	2
2011	2	-	-	1	1

Källa: Brå

9.2.6 Sammanfattande kommentar

När det gäller de redovisade statistikuppgifterna kan bl.a. konstateras följande.

Antalet anmälda dataintrång har ökat mycket de senaste åren: från 731 år 2003 till 8 646 år 2012, vilket innebär en ökning med nästan 1 100 procent under denna tioårsperiod.

En svaghet i de statistiska uppgifterna ligger i det förhållandet att dataintrångsbestämmelsen omfattar en mängd olika typer av förfaranden av varierande grad av allvar men att dataintrång enbart representeras av en enskild brottskod i den officiella kriminalstatistiken. Det är alltså omöjligt att av statistiken utläsa vilken typ av dataintrångsgärning en viss anmälan avsett och om den stora ökningen av antalet anmälda dataintrång avser en viss typ av gärning.

Andelen personuppklarade dataintrång, dvs. fall där en gärningsman kunnat knytas till brottet, är låg och ligger på i genomsnitt drygt 6 procent de senaste tio åren.

Påföljden för dataintrång eller brytande av post- eller telehemlighet som huvudbrott har inte i något fall under tioårsperioden 2002–2011 bestämts till fängelse och den vanligaste påföljden har varit böter.

[5] Skyddstillsyn/Villkorlig dom (i förekommande fall i kombination med samhällstjänst).
[6] Andra påföljder än de särskilt redovisade och åtalsunderlåtelse.

Antalet lagföringar när det gäller brytande av post- eller telehemlighet har varit ytterst få.

En förklaring till att andelen personuppklarade dataintrång varit låg kan vara att leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster fram till den 1 juli 2012 enbart var skyldiga att lämna ut uppgifter om abonnemang beträffande misstanke om brott som bedömdes kunna föranleda annan påföljd än böter. Som framgått har den vanligaste påföljden för dataintrång de senaste åren varit böter, varför det i viss utsträckning kan ha varit tekniskt svårt att utreda dessa brott.

När det gäller dataintrång kan vidare befaras att mörkertalet är betydande och att statistiken över anmälda dataintrång inte ger en rättvisande bild av hur många brott som faktiskt begåtts ett visst år. Enligt uppgifter som vi inhämtat är företag som utsatts för olika former av dataintrång – överbelastnings- tillgänglighets- eller intrångsattacker – inte sällan rädda för de skadeverkningar och negativa effekter i form av minskat förtroende för och minskad efterfrågan av deras tjänster som publicitet om att de utsatts för en attack kan leda till. Rädslan för publicitet medför att brottet inte anmäls. Uppfattningen från polis- och åklagarhåll är även att anmälningsfrekvensen generellt sett är låg när det gäller dataintrång.

9.3 Behovet av ändrade straffskalor

Bedömning: Det finns ett behov av skärpta straff för dataintrång. Motsvarande behov finns inte när det gäller brytande av post- eller telehemlighet.

Skälen för bedömningen

Allmänna utgångspunkter vid utformning av straffskalor

Utgångspunkterna såväl vid utformning av straffskalor som vid straffmätning i domstol är principerna om *proportionalitet* och *ekvivalens*. De straffteoretiska grunderna för påföljdssystemet har beskrivits och diskuterats i flera lagstiftningsarbeten på straffrättens område (se bl.a. Fängelsestraffkommittén, *Påföljd för brott*, SOU 1986:13–15, som behandlas i prop. 1987/88:120, Straffsystemkommittén, *Ett reformerat straffsystem*, SOU 1995:91, som behandlas i prop. 1997/98:96

och Straffnivåutredningens betänkanden, *Straffskalan för mord*, SOU 2007:90, och *Straff i proportion till brottets allvar*, SOU 2008:85, som behandlas i prop. 2008/09:118 respektive 2009/10:147).

I korthet innebär proportionalitets- och ekvivalensprinciperna att straff ska motsvara brottets svårhet. Svårare brott ska bestraffas strängare än lindrigare brott och brott som är lika svåra ska bestraffas lika strängt. Det straff som en domstol i det enskilda fallet dömer ut visar således hur allvarlig gärningen är i förhållande till andra brott. På samma sätt ger ett brotts straffskala en indikation om hur allvarligt det brottet är i förhållande till andra brott.

Dataintrång

Dataintrångsbestämmelsen har samma straffskala som när bestämmelsen först infördes i datalagen (1973:289) i samband med den lagens tillkomst. Straffskalan har alltså varit oförändrad under fyrtio års tid. Under denna tid har det skett en betydande samhällsutveckling och informationssystem har i dag en ojämförligt större betydelse i samhället än för fyrtio år sedan. Informationssystemen är i stor utsträckning sammankopplade, vilket medför att angrepp lätt kan få långtgående konsekvenser.

Myndigheter, företag och organisationer är i hög grad beroende av informationssystem och använder i stor utsträckning datorer och datasystem anslutna till lokala datanät, vilka i sin tur ofta är anslutna till större företagsnät eller internet. Många företag, inte minst inom den finansiella sektorn, baserar hela sin verksamhet på internet och internet används även som infrastruktur för styrning av processer inom industrin. Även samhällsviktig infrastruktur är beroende av datasystem, datanät, elektroniska kommunikationer och internet för en rad funktioner. Den offentliga sektorn har ökat sitt internetberoende bl.a. i och med satsningar på självbetjäningstjänster och 24-timmarsmyndigheter. Elektroniska kommunikationer och internet är därmed i dagens samhälle av stor betydelse för såväl företagens affärstransaktioner som statens möjligheter att tillhandahålla tjänster till medborgarna. Informationssystem är av avgörande betydelse för människors vardag, vilket bl.a. det stora antal betalningar som allmänheten gör via internet visar på. Tilliten till och förtroendet för elektroniska kommunikationstjänster och internet är därmed av betydande vikt.

Post- och telestyrelsen (PTS), som av regeringen fått i uppdrag att lämna förslag på en strategi för ett säkrare internet i Sverige, har konstaterat att det, i takt med att samhället blir allt mer beroende av it i allmänhet och internet i synnerhet, blir allt mer intressant för organiserad brottslighet att angripa samhället genom systematiska tekniska attacker i stället för via mer traditionella medel (PTS rapport *Strategi för ett säkrare Internet i Sverige*, 2006, PTS-ER-2006:12, s. 24–25). Attackerna utförs, enligt PTS, inte längre enbart av enstaka hackare som vill testa sin förmåga, utan även av mer organiserade grupperingar som har ekonomisk vinning som syfte eller som har ideologiska motiv.

För varje nät eller system som är anslutet till internet finns en risk att drabbas av olika former av angrepp så som datavirus, e-postvirus, trojaner, försök till intrång, intrång och överbelastningsattacker. Angreppen kan medföra synnerligen allvarliga konsekvenser för den verksamhet som drabbas. Till synes kan angreppen i princip drabba vilka nät och datasystem som helst. Risken för sådana angrepp kan ses som ett ”*bakgrundshot*” för nät och datorer anslutna till internet (se PTS utredning *Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering*, 28 november 2000, s. 23).

Myndigheter, företag och organisationer kan också utsättas för *riktade angrepp*, dvs. angrepp som avsiktligt är riktade mot ett visst mål. Exempel på sådana angrepp är överbelastnings- eller tillgänglighetsattacker som antingen utförs av enstaka angripare eller genom att många användare mobiliseras för angrepp, i syfte att skada det angripna målet. Angripare kan exempelvis försöka uppnå att målets verksamhet störs för att påverka dess affärsverksamhet eller för att sabotera en verksamhet som man ogillar av det ena eller andra skälet. Angrepp i form av intrångsattacker eller andra typer av angrepp kan också riktas mot myndigheter, företag och organisationer i syfte att tillskansa angriparna egen vinning och som ett led i andra brott, exempelvis olika former av bedrägerier eller utpressning, riktade mot den angripna personen (se PTS utredning *Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering*, 28 november 2000, s. 24 och 32). Angreppen kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och kommunikation. De kan också leda till förlust eller förvanskning av hemlig eller i övrigt integritetskänslig information.

Som tidigare framhållits är det med hänsyn till den stora betydelse som informationssystem har i dagens samhälle av vikt att förtroendet för elektroniska kommunikationstjänster kan upprätthållas.

Omfattande angrepp mot informationssystem kan, förutom de verkningar som tidigare nämnts – dvs. omfattande ekonomiska skador och förlust eller förvanskning av information – få konsekvenser som är svåra att överblicka. Överbelastningsattacker eller andra former av angrepp eller intrång mot en eller flera banker skulle kunna få till följd att ett helt bank- eller betalningssystem kollapsade. Även om följderna inte skulle bli fullt så dramatiska skulle ett angrepp av det slaget kunna orsaka stora samhällskostnader.

Mot bakgrund av den betydelse som informationssystem har i dagens samhälle och de synnerligen stora skador, ekonomiska eller av andra slag, som ett angrepp mot informationssystem kan orsaka är det lätt att tänka sig fall där en sådan gärning, om man tar de straffteoretiska principerna om proportion och ekvivalens som utgångspunkt, har ett straffvärde som är betydligt högre än fängelse två år. Till sina verkningar skulle angrepp av det beskrivna slaget kunna jämföras med grov skadegörelse eller sabotage.

Som vi närmare redogjort för i avsnitt 7.3.7 kan i vissa fall av angrepp mot informationssystem ansvar för grov skadegörelse, sabotage, grovt sabotage och terroristbrott komma i fråga. Dessa straffbestämmelser ger möjlighet till utdömande av högre straff. Straffskalan för grov skadegörelse är fängelse i högst fyra år. Straffskalorna för sabotage och grovt sabotage är fängelse i högst fyra år respektive fängelse på viss tid, lägst två och högst tio år, eller på livstid. För terroristbrott är straffet fängelse på viss tid, lägst fyra och högst 18 år, eller på livstid. Är brottet mindre grovt, är straffet fängelse, lägst två år och högst sex år. Det kan emellertid tänkas en rad situationer där det, trots att gärningen medfört stora ekonomiska skador på grund av avbrott i informationssystems drift och kommunikation, inte är möjligt att tillämpa skadegörelse-, sabotage-, och terroristbrottsbestämmelserna, exempelvis för att skadan är av tillfällig karaktär eller för att inte sådan för samhället viktig egendom som avses i sabotagebestämmelsen skadats.

I den tidigare beskrivna situationen med överbelastningsattacker eller andra former av angrepp eller intrång mot en eller flera banker är det mycket tveksamt om någon annan straffbestämmelse än dataintrångsbestämmelsen skulle bli tillämplig, trots att angreppet fått vittgående konsekvenser.

Som framgår av den tidigare redovisade kriminalstatistiken har antalet anmälda dataintrång ökat markant de senaste åren och trenden visar på en fortsatt ökning. Den redovisade statistiken i fråga om val av påföljd, som visar att straffvärdet endast i ett fåtal fall har

ansetts överstiga böter när huvudbrottet varit dataintrång, indikerar enligt vår mening att dataintrångsbrottets farlighet och skadlighet inte har värderats tillräckligt. I några tings- och hovrättsdomar som vi har gått igenom, där gärningsmännen dömts för relativt allvarliga former av dataintrång och där skadeverkningarna antingen blivit eller i vart fall kunnat bli förhållandevis allvarliga skulle enligt vår mening gärningarna kunna anses ha ett högre straffvärde än vad domstolarna har kommit fram till. Vår uppfattning är att det även för sådana dataintrångsgärningar som ryms inom den befintliga straffskalan finns ett allmänt behov av att göra en mer differentierad bedömning av straffvärdet och i större utsträckning utnyttja spännvidden i straffskalan. Dataintrångsbestämmelsen inrymmer en mängd olika förfaranden av varierande grad av allvar. Vissa av dem motiverar inte annan påföljd än böter, vissa har ett straffvärde i paritet med allvarligare former av grov skadegörelse och sabotage och vissa, slutligen, har ett straffvärde någonstans där emellan.

Beroendet av elektroniska informationssystem och internet ökar ständigt och som en konsekvens av det blir samhället allt mer mottagligt för it-angrepp. Det finns tecken på att utvecklingen går mot allt farligare och mer storskaliga angrepp mot informationssystem, till exempel intrång i eller överbelastningsattacker mot bankers och myndigheters informationssystem. Överbelastningsattackerna mot ett antal svenska myndigheter och organisationer inom bl.a. banksektorn och media i oktober 2012 är ett exempel på detta. Drabbade myndigheter och organisationer fick sina webbplatser temporärt otillgängliga under de perioder attackerna pågick. I några fall drabbades webbplatser av upprepade attacker, och i åtminstone ett fall lyckades angripare göra intrång i en webbserver och byta ut information på en myndighets hemsida. Några allvarligare dataintrång kunde emellertid inte kopplas till attackerna och konsekvenserna begränsades till att de drabbade webbplatserna inte kunde nås. Skadeeffekterna var därmed svårvärderade och bestod i huvudsak i minskad servicegrad och i några fall i bortfall av potentiella intäkter samt eventuell negativ publicitet (se Myndigheten för samhällsskydd och beredskap [MSB], PM, 2012-11-06, diarienr 2012-5642). Riktade intrångsförsök mot svenska intressen har även skett vid tidigare tillfällen. Intrångsförsöken har bl.a. utförts genom att individuellt anpassad e-post sänts till individer inom den utsatta organisationen. Breven har sett ut att ha trovärdiga avsändare som förefallit rimliga i förhållande till brevens innehållstext och texten har varit relevant för det arbetsområde mottagaren verkat inom. Med breven har följt

bilagor, vilka om de öppnats infekterat mottagarens dator med en medföljande skadlig kod, alternativt har meddelandetexten innehållit länkar som lett till webbplatser som infekterar mottagarens dator. Den skadliga kod som installeras på den drabbade maskinen gör det möjligt för angriparen att utifrån ta kontroll över maskinen och på så sätt uppstår en risk att information hämtas ut från den drabbade maskinen (MSB:s nyhetsbrev 2006-04-07).

Dataintrångbestämmelsens nuvarande straffskala, som sträcker sig från böter till fängelse två år, ger enligt vår uppfattning inte tillräckligt utrymme för att i överensstämmelse med brottsbalkens principer om olika gärningars relativa proportionalitet kunna beakta allvaret i storskaliga angrepp mot informationssystem. Som vi tidigare har konstaterat är det av olika skäl inte alltid möjligt att vid sådana angrepp mot informationssystem tillämpa andra straffbestämmelser med högre straffskalor, såsom bestämmelserna om sabotage, grov skadegörelse och terroristbrott. Uppfattningen att straffskalan för dataintrång bör skärpas har under senare år framförts av olika myndigheter i annat sammanhang (se exempelvis Rikspolisstyrelsens, Säkerhetspolisens och Göteborgs tingsrätts remissyttranden över promemorian *Angrepp mot informationssystem* [Ds 2005:5]). Regeringen har då gjort bedömningen att en ändring av straffskalan för dataintrång eller ett införande av ett grovt sådant brott förutsatte en analys som det saknades beredningsunderlag för och som inte heller var möjlig att göra inom ramen för det aktuella lagstiftningsärendet (prop. 2006/07:66 s. 30).

Vi har tidigare gjort bedömningen att det för att uppfylla direktivets bestämmelser om straffskalornas utformning när det gäller brotten olaglig systemstörning och olaglig datastörning finns behov av att skärpa straffskalan för dataintrång (se avsnitt 7.3.7). Enligt vår mening finns det vid sidan av direktivet andra kriminalpolitiska skäl för detta.

Brytande av post- eller telehemlighet

Bestämmelsen om brytande av post- eller telehemlighet har haft samma straffskala sedan brottsbalkens tillkomst år 1962.

Bestämmelsen skyddar såväl meddelanden i traditionell form som elektroniska meddelanden och omfattar intrång i den sist nämnda typen av meddelanden oavsett på vilket sätt dessa tekniskt förmedlas, med visst undantag för meddelanden som befordras via radio.

Skyddet sträcker sig från den tidpunkt när meddelandet har avlämnats för befordran till dess att meddelandet har nått mottagaren. I den mån meddelanden i ett elektroniskt kommunikationsnät befordras på annat sätt än via ett telebefordringsföretag, exempelvis via privata kommunikationsnät, skyddas de inte av straffbestämmelsen. Den brottsliga gärningen består i att bereda sig tillgång till meddelandet.

Av den redovisade kriminalstatistiken framgår att antalet lagföringar när det gäller brytande av post- eller telehemlighet har varit ytterst få under den redovisade tioårsperioden. Av statistiken framgår inte hur många – om ens någon – av lagföringarna som avsett intrång i elektroniska meddelanden.

Bestämmelsen om brytande av post- eller telehemlighet syftar till att bereda straffrättsligt hemlighetsskydd för befordran av postförsändelser och elektroniska meddelanden (NJA II 1962 s. 135 och Berggren m.fl., *Brottsbalken En kommentar kap. 1–12*, s. 4:34). Rätten att fritt och utan obehörigt intrång kunna skicka såväl traditionella som elektroniska meddelanden anses höra till medborgarnas personliga frihet och det är av vikt att det finns ett straffrättsligt skydd mot angrepp på denna rätt. Det är emellertid svårt att se att det förfarande som bestämmelsen om brytande av post- eller telehemlighet straffbelägger skulle kunna orsaka motsvarande skada och få så vittgående konsekvenser som vissa av de förfaranden som dataintrångsbestämmelsen straffbelägger och som har beskrivits i föregående avsnitt. Sådana storskaliga angrepp mot informationssystem som det finns ett behov av att kunna utdöma hårdare straff för, i den mån de inte träffas av sabotage- och skadegörelsebestämmelserna, omfattas inte av bestämmelsen om brytande av post- eller telehemlighet utan av dataintrångsbestämmelsen. Möjligtvis skulle, som en del i ett storskaligt angrepp, intrång kunna göras i ett elektroniskt meddelande under befordran i syfte att få del av information som behövs för det planerade angreppet. Det är emellertid inte då den del av förfarandet som avser brytandet av telehemligheten som åstadkommer den stora skadan, utan senare delar som är straffbelagda enligt bestämmelserna om dataintrång, skadegörelse, sabotage eller terroristbrott.

Straffskalan för brytande av post- eller telehemlighet sträcker sig från böter till fängelse två år. Enligt vår mening är den nuvarande straffskalan alltjämt väl avvägd. Att den tekniska utvecklingen inneburit att bestämmelsen, sett till *antal* meddelanden som befordras, i dag säkerligen skyddar långt fler elektroniska än traditionella med-

delanden, påverkar inte denna bedömning. Skyddsintresset är fortfarande hemligheten i de meddelanden som befordras och detta blir inte starkare eller svagare beroende på vilket sätt som meddelandet befordras på. En oförändrad straffskala för brytande av post- eller telehemlighet innebär att denna också i fortsättningen är densamma som för intrång i förvar (4 kap. 9 §) och olovlig avlyssning (4 kap. 10 §). Enligt vår uppfattning är det riktigt eftersom samtliga dessa bestämmelser i princip avser att skydda samma intresse – integriteten i olika former av kommunikationer – och samtliga dessa brottstyper får anses lika allvarliga. Om någon exempelvis olovligen öppnar ett brev som är under befordran är gärningen straffbar som brytande av posthemlighet medan om samma brev öppnas sedan det lämnats i adressatens brevlåda är gärningen straffbar som intrång i förvar. Det finns inte anledning att ha olika straffskalor beroende på sättet som hemligheten bryts på.

För uppfyllande av kraven i direktivet är brottet brytande av post- eller telehemlighet enbart av betydelse för direktivets artikel 6 om olaglig avlyssning (se avsnitt 7.3.4). Direktivet ställer inte högre krav på straffskalan för olaglig avlyssning än att denna gärning ska ha en straffskala med ett maximistraff på minst två års fängelse (se artikel 9.2 och avsnitt 7.3.7). Följaktligen uppfyller svensk rätt redan direktivets krav i detta avseende.

Enligt vår uppfattning finns alltså inte, varken mot bakgrund av direktivet eller vid sidan av detta, skäl att skärpa straffet för brytande av post- eller telehemlighet.

9.4 En särskild straffskala för grovt dataintrång

Förslag: En särskild straffskala för grovt dataintrång införs. Straffskalan ska sträcka sig från fängelse sex månader till fängelse sex år.

Vid bedömande av om ett dataintrång är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art.

Bestämmelsen om dataintrång ska inte längre vara subsidiär i förhållande till straffbestämmelserna om brytande av post- eller telehemlighet och om intrång i förvar.

Försök och förberedelse till grovt dataintrång ska vara straffbart.

Skälen för förslaget

Inledning

Vi har i tidigare avsnitt gjort bedömningen att det för att uppfylla direktivets bestämmelser om straffskalornas utformning när det gäller brotten olaglig systemstörning och olaglig datastörning finns behov av att skärpa straffskalan för dataintrång (se avsnitt 7.3.7).

I föregående avsnitt har vi konstaterat att det även finns självständiga skäl att skärpa straffet för dataintrång.

Förändring av straffskalan eller särskild straffskala för grovt brott?

Den grundläggande utgångspunkten för utformning av straffskalor är, som nämnts i tidigare avsnitt, brottets allvar. Straffskalan för ett brott ska återspegla hur allvarligt eller klandervärt brottet är. Ett allvarligt brott ska bestraffas strängare än ett mindre allvarligt brott och lika allvarliga brott ska bestraffas lika strängt.

Den nuvarande straffskalan för dataintrång sträcker sig från böter till fängelse två år. Straffbestämmelsen omfattar en mängd olika typer av förfaranden av varierande grad av allvar. Straffstadgandet innefattar alltså gärningar av mycket olika straffvärde och straffskalan måste vara utformad på ett sådant sätt att den medger en nyanserad bedömning av straffvärdet i enlighet med de nämnda principerna om proportionalitet och ekvivalens.

För en rad av de förfaranden som straffbeläggs som dataintrång, exempelvis vissa fall då någon gjort en otillåten slagning i ett datasystem på arbetet, på annat sätt enbart berett sig tillgång till en uppgift i ett datasystem utan att något skadats eller att någon säkerhetsåtgärd kringgåtts eller mindre allvarliga fall av kapning av ett Facebook-konto eller falska statusuppdateringar på Facebook eller andra konton på sociala medier (s.k. facerapes), är den nuvarande straffskalan fullt tillräcklig och för de förfaranden som nyss nämnts kan böter säkerligen i många fall vara en adekvat påföljd för brottet. Som brottstyp betraktat är det inte heller allvarligare att olovligen bereda sig tillgång till ett elektroniskt meddelande som är under befordran i ett privat kommunikationsnät än att olovligen bereda sig tillgång till ett elektroniskt meddelande som är under befordran via ett telebefordringsföretag. Straffminimum för dataintrång bör mot den bakgrunden vara densamma som för brytande av post-

eller telehemlighet. Enligt vår uppfattning är det alltså inte aktuellt att föreslå en höjning av straffminimum för dataintrångsbrottet.

Vår uppfattning är att det inte heller finns någon anledning att föreslå en ringa form av dataintrång. Böter ingår redan i straffskalan för dataintrång och det är, mot bakgrund av vad som nyss sagts, rimligt att straffskalan för de minst allvarliga fallen av dataintrång harmonierar med den som gäller för brytande av post- eller telehemlighet.

Enligt artikel 9.3 i direktivet ska brotten olaglig systemstörning och olaglig datastörning ha ett lägsta maximistraff på tre års fängelse när ett betydande antal informationssystem har påverkats genom användning av ett verktyg som har utformats primärt för detta syfte. Enligt artikel 9.4 ska vidare brotten olaglig systemstörning och olaglig datastörning ha ett lägsta maximistraff på fem års fängelse när de a) begås inom ramen för en kriminell organisation, b) förorsakar allvarlig skada, eller c) begås mot ett kritiskt infrastruktursystem. Svensk rätt uppfyller genom främst dataintrångsbestämmelsen direktivets krav på vilka handlingar som ska vara straffbelagda som olaglig systemstörning och olaglig datastörning. Vissa av de gärningar som nämns i artikel 9.3 och 9.4 kan även tänkas motsvara andra brott i svensk rätt, främst skadegörelse och sabotage, men långt ifrån alla. Mot den bakgrunden måste straffet för vissa former av dataintrång skärpas till minst fem års fängelse för att svensk rätt ska uppfylla direktivets krav i fråga om påföljder.

Att inom ramen för en och samma straffbestämmelse ha en straffskala som sträcker sig från böter till fem års fängelse eller mer är enligt vår uppfattning inte lämpligt. Det skapar helt enkelt en för stor spänning i straffskalan. En sådan vid straffskala skulle också innebära att även dataintrång med lågt straffvärde, som inte motiverar annat än ett bötesstraff, skulle få en förlängd preskriptionstid på minst tio år. En sådan konsekvens är enligt vår mening inte rimlig. I stället föreslår vi i enlighet med svenska principer för straffrättslig lagstiftning en särskild straffskala för grovt dataintrång.

Genom att föreskriva en särskild straffskala för de allvarligaste fallen av dataintrång är det också möjligt att peka ut de omständigheter som bör leda till en strängare bedömning än annars.

Att enbart höja straffskalan för dataintrång och inte införa en särskild straffskala för grovt brott skulle även innebära att straffmaximum för dataintrång generellt skulle vara högre än straffmaximum för brytande av post- eller telehemlighet och intrång i förvar. Konsekvensen skulle alltså bli att brottstypen dataintrång

skulle anses allvarligare än de andra två brottstyperna. Så kan emellertid inte generellt anses vara fallet. Många av de förfaranden som träffas av dataintrångbestämmelsen har samma grad av allvar som de som träffas av bestämmelserna om brytande av post- eller telehemlighet och intrång i förvar (jfr den tidigare jämförelsen om att olovligen bereda sig tillgång till ett elektroniskt meddelande som är under befordran i ett privat kommunikationsnät respektive via ett telebefordringsföretag). Att det finns behov av skärpta straff för dataintrång beror på att det brottet i vissa fall kan bestå i storskaliga eller av andra skäl särskilt farliga angrepp mot informationssystem som kan orsaka betydande ekonomiska skador eller skador av annat slag. Som tidigare har konstaterats behövs vidare en skärpt straffskala för dataintrång för att genomföra direktivet.

Vilka omständigheter bör tillmätas särskild vikt vid bedömande av om ett dataintrång är grovt?

När en särskild straffskala för grovt dataintrång införs bör det på det sätt som är vanligt i svensk straffrätt anges vilka omständigheter som särskilt ska beaktas vid bedömningen av om brottet är grovt. En sådan utformning leder normalt till bättre förutsebarhet och till större enhetlighet i rättstillämpningen (jfr prop. 2011/12:109 s. 16). Avsikten är inte att *endast* de omständigheter som lyfts fram i bestämmelsen ska beaktas eller att de alltid ska leda till en användning av den strängare straffskalan. En helhetsbedömning ska göras av *samtliga* omständigheter i det enskilda fallet, varvid såväl försvårande som förmildrande omständigheter ska beaktas.

Frågan är då hur bestämmelsen närmare bör utformas. När det gäller vilka omständigheter som bör anges i bestämmelsen bör hänsyn tas till EU-direktivets artikel 9.3 och 9.4. I dessa anges vissa lägsta maximistraff för brott som i svensk rätt i huvudsak motsvaras av dataintrång när vissa uppräknade omständigheter föreligger. De omständigheter som anges är 1) att ett betydande antal informationssystem har påverkats genom användning av vissa verktyg, exempelvis olika former av sabotageprogram (artikel 9.3) eller att brotten 2) begås inom ramen för en kriminell organisation, 3) förorsakar allvarlig skada, eller 4) begås mot ett kritiskt infrastruktursystem (artikel 9.4).

Att dataintrånget inneburit att ett stort antal informationssystem har påverkats, exempelvis genom en överbelastnings- eller tillgäng-

lighetsattack, bör enligt vår mening kunna utgöra grund för att ett dataintrång bedöms som grovt. Det är typiskt sett en sådan omständighet som, mot bakgrund av den stora betydelse som informationssystem har i dagens samhälle och den tillit till systemen som detta förutsätter, kan få allvarliga konsekvenser, såväl för enskilda företag och banker som för statliga myndigheter. Även andra former av storskaliga attacker som inte innebär att själva systemet påverkas utan att uppgifterna i systemet exempelvis raderas eller ändras bör kunna utgöra grund för att ett dataintrång bedöms som grovt.

Det objekt som skyddas genom dataintrångsbestämmelsens nuvarande utformning är uppgift som är avsedd för automatiserad behandling. Utgångspunkten är alltså att det är *uppgiften* som är det skyddsvärda. En bestämmelse om grovt dataintrång bör utformas i enlighet med detta grundläggande synsätt. Mot den bakgrunden anser vi att bestämmelsen bör utformas så att den ger möjlighet att beakta att gärningen har avsett ett stort antal uppgifter. Omfattande tillgänglighets- eller överbelastningsattacker liksom stor spridning av virusprogram eller andra sabotageprogram är exempel på gärningar av detta slag. Ett annat exempel är då en betydande mängd uppgifter har manipulerats på något av de sätt som sägs i första stycket eller då någon berett sig tillgång till en stor mängd uppgifter. En sådan utformning innebär alltså att den omständighet som anges i direktivets artikel 9.3 fångas upp som försvårande och särskilt bör beaktas vid bedömningen av om brottet är grovt.

Ytterligare en omständighet som bör beaktas som försvårande är om gärningen har orsakat eller kunnat orsaka allvarlig skada. Att brottet orsakar allvarlig skada är, som framgått, en omständighet som även tas upp i direktivet. Gärningens skadeverkningar bör, om de är tillräckligt omfattande, ensamt kunna kvalificera brottet som grovt, oavsett övriga omständigheter under förutsättning här som annars att den skada som orsakats eller kunnat orsakas täcks av gärningsmannens uppsåt.

Den skada som vi avser är främst sådan som är av ekonomisk natur, men även skada av annat slag, exempelvis sådan ideell skada som kan uppkomma vid intrång i informationssystem som innehåller integritetskänslig information, omfattas.

Som särskild omständighet att beakta vid bedömande av om ett dataintrång är grovt bör slutligen anges att gärningen varit av särskilt farlig art. Genom denna omständighet täcks sådana förfaranden in där det kan vara svårt att avgöra hur omfattande skadan blivit

eller kunnat bli, men där själva förfarandet i sig fått eller kunnat få långtgående konsekvenser. Som exempel på sådana förfaranden skulle kunna nämnas intrång i myndigheters datasystem med uppgifter om personer med skyddad identitet eller attacker som i förlängningen skulle kunna leda till en kollaps av betalningssystemet. Även det förhållande som anges i direktivets artikel 9.4, att brottet begås mot ett kritiskt infrastruktursystem, täcks enligt vår mening in av omständigheten att gärningen varit av särskilt farlig art. Som nämnts i avsnitt 7.3.7 kan dock gärningar som begås mot kritiska infrastruktursystem i många fall även omfattas av den svenska sabotagebestämmelsen.

I direktivets artikel 9.4 anges även, som framgått, att en sådan omständighet som ska kunna medföra att brott som i svensk rätt i huvudsak motsvaras av dataintrång ska vara belagda med visst maximistraff är att brotten begås inom ramen för en kriminell organisation. Enligt svensk rätt ska som en försvårande omständighet vid bedömningen av ett brotts straffvärde i allmänhet beaktas om brottet utgjort ett led i en brottslighet som utövats i organiserad form eller systematiskt eller om brottet föregåtts av särskild planering (29 kap. 2 § 6 brottsbalken). Detta ger enligt vår mening tillräckligt utrymme för att beakta att gärningen begåtts inom ramen för en kriminell organisation.

Direktivets artikel 9.5 ställer krav på att det ska kunna anses som en försvårande omständighet när brott som i svensk rätt i huvudsak motsvaras av dataintrång begås genom missbruk av personuppgifter. Enligt vår mening finns utrymme att inom ramen för 29 kap. 2 § brottsbalken beakta denna omständighet som försvårande (jfr avsnitt 7.3.7).

Vilken straffskala bör gälla för grovt dataintrång?

Straffet för grovt dataintrång måste vara minst fem års fängelse för att svensk rätt i alla delar ska uppfylla direktivets krav i fråga om påföljder. Ett maximistraff på fem års fängelse passar mindre väl in i den svenska systematiken när det gäller utformningen av straffskalor. Frågan är också om ett maximistraff på fem års fängelse är tillräckligt för att en adekvat bedömning av straffvärdet ska kunna göras vid de mest allvarliga formerna av dataintrång. Som framhållits i avsnitt 9.3 kan omfattande angrepp mot informationssystem skapa en allmän osäkerhet om huruvida det går att känna tilltro till

viktiga samhällsfunktioner, bl.a. myndigheters och bankers datasystem och tjänster. De skadeverkningar som ett dataintrång kan orsaka liknar därför de skadeverkningar som kan orsakas av sådana gärningar som träffas av bestämmelsen om sabotage och i vissa fall även av grovt sabotage. Grovt sabotage är dock som brottstyp att anse som ett allvarligare brott än grovt dataintrång. Mot den bakgrunden föreslår vi ett maximistraff på sex års fängelse.

Straffskalorna för dataintrång av normalgraden och grovt dataintrång bör vara något överlappande. Med detta menas att en viss del av straffskalan för en grad av ett brott är gemensam med straffskalan för en annan grad av brottet. Om straffskalan för grovt dataintrång bestäms till fängelse i lägst sex månader och högst sex år, blir överlappningen mellan straffskalorna jämförlig med hur överlappningen utformats vid jämförbara gradindelade brott. Exempel på andra brott i brottsbalken med helt motsvarande gradindelade straffskalor är olaga tvång/olaga tvång som är grovt (4 kap. 4 §), trolöshet mot huvudman/trolöshet mot huvudman som är grovt (10 kap. 5 §) och utnyttjande av barn för sexuell posering/grovt utnyttjande av barn för sexuell posering (6 kap. 8 §).

Även stöld/grov stöld, bedrägeri/grovt bedrägeri, häleri/grovt häleri och förskingring/grov förskingring har en motsvarande överlappning, men där ingår inte böter i straffskalan för stöld, bedrägeri, häleri och förskingring eftersom det finns särskilda ringa former av dessa brott genom bestämmelserna om snatteri, bedrägligt beteende, häleriförseelse och undandräkt (8 kap. 1, 2 och 4 §§, 9 kap. 1–3 §§, 9 kap. 6 och 7 §§ respektive 10 kap. 1–3 §§). Vi har tidigare angett att vi inte anser att det finns skäl att införa en särskild ringa form av dataintrång.

Som tidigare nämnts innefattar dataintrångsbestämmelsen gärningar av mycket olika straffvärde. En utformning av straffskalan för grovt dataintrång i enlighet med vad som nyss sagts innebär enligt vår mening att straffskalan medger en adekvat bedömning av straffvärdet för olika former av dataintrång. En sådan utformning innebär också att svensk rätt i alla delar uppfyller direktivets krav i fråga om påföljder. Utformningen passar slutligen väl in i brottsbalkens systematik när det gäller gradindelade brott.

Vi föreslår alltså att straffskalan för grovt dataintrång bestäms till fängelse lägst sex månader och högst sex år.

Försök och förberedelse till grovt dataintrång bör vara straffbart. Mot bakgrund av den restriktivitet som finns i svensk rätt att

straffbelägga brott redan på stämplingsstadiet anser vi däremot inte att stämpling till grovt dataintrång bör vara straffbart.

Förhållandet mellan dataintrångsbestämmelsen och bestämmelserna om brytande av post- eller telehemlighet och intrång i förvar

Den nuvarande ordningen innebär att dataintrångsbestämmelsen är subsidiär i förhållande till bestämmelserna om brytande av post- eller telehemlighet och intrång i förvar. Skälen för den uttryckliga subsidiaritetsregeln angavs inte i samband med att den infördes då dataintrångsbestämmelsen utan ändring i sak fördes över från datalagen (1973:289) till brottsbalken (prop. 1997/98:44 s. 113 och 149). Som vi tidigare har redovisat ser vi inte något behov av att, på det sätt som vi föreslår när det gäller dataintrång, lämna förslag till skärpta straff för brytande av post- eller telehemlighet.

Enligt vårt förslag ska straffskalan för dataintrång av normalgraden vara densamma som för brytande av post- eller telehemlighet och intrång i förvar, dvs. böter eller fängelse i högst två år. Samtidigt införs en särskild straffskala för grovt dataintrång som sträcker sig från fängelse sex månader till fängelse sex år. Det leder till att dataintrångsbestämmelsens subsidiaritet inte bör behållas. Vi återkommer till olika konkurrensfrågor i författningskommentaren.

Andra konsekvenser

Ett införande av en särskild straffskala för grovt dataintrång som sträcker sig från fängelse sex månader till fängelse sex år får också andra konsekvenser än sådana som är hänförliga till straffmätningen, bl.a. när det gäller möjligheterna att tillgripa vissa straffprocessuella tvångsmedel. Generellt gäller att möjligheterna till tvångsmedelsanvändning ökar ju högre straffvärde brottet har.

Hemlig avlyssning av elektronisk kommunikation får användas 1) vid förundersökning som avser ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller 2) försök, förberedelse eller stämpling till ett sådant brott, om sådan gärning är belagd med straff, samt 3) vid förundersökning som gäller ett brott med lägre straffminimum, om brottets straffvärde bedöms överstiga fängelse i två år (27 kap. 18 § andra stycket rättegångsbalken).

Enligt straffvärdeventilen i den tredje punkten behöver alltså minimistraffet inte vara fängelse två år för att hemlig avlyssning av elektronisk kommunikation ska få beslutas. Bestämmelsen är enligt förarbetena tillämplig även vid osjälvständiga brott (prop. 2002/03:74 s. 34–35). Även försök, förberedelse och stämpling – i den utsträckning dessa osjälvständiga brottsformer är straffbara – omfattas alltså av straffvärdeventilen.

Motsvarande förutsättningar som gäller för hemlig avlyssning av elektronisk kommunikation gäller för användning av hemlig kameraövervakning (27 kap. 20 a § andra stycket rättegångsbalken).

Med den utformning av straffskalan för grovt dataintrång som vi föreslår, blir det möjligt att besluta om hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning vid misstanke om grovt dataintrång eller försök eller förberedelse till sådant brott under förutsättning att domstolen gör bedömningen att brottets straffvärde är högre än två år.

Hemlig övervakning av elektronisk kommunikation får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader och vid förundersökning om vissa särskilt angivna brott (27 kap. 19 § andra stycket rättegångsbalken). Dataintrång är ett sådant särskilt angivet brott, varför möjligheterna att besluta om hemlig övervakning av elektronisk kommunikation vid misstanke om dataintrång inte direkt påverkas av vårt förslag.

Ett införande av en särskild straffskala för grovt dataintrång får även betydelse för frågan om preskription av brott. Med nuvarande straffskala innebär regleringen i 35 kap. 1 § brottsbalken att påföljd inte får dömas ut för dataintrång om inte den misstänkte har häktats eller har fått del av åtal för brottet inom fem år från den dag det begicks. Förslaget om en särskild straffskala för grovt dataintrång innebär att preskriptionstiden för sådana fall av dataintrång som bedöms som grova kommer att bli tio år.

De konsekvenser av att en särskild straffskala för grovt dataintrång införs som här redogjorts för bedömer vi som rimliga.

10 Konsekvenser av förslagen

10.1 Inledande anmärkningar

Enligt 14–15 a §§ kommittéförordningen (1998:1474) ska varje utredning beräkna och redovisa i vad mån dess förslag

- påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda,
- innebär samhällsekonomiska konsekvenser i övrigt,
- har betydelse för den kommunala självstyrelsen, brottsligheten och det brottsförebyggande arbetet, sysselsättning och offentlig service i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, eller
- har betydelse för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

När det gäller förslag som innebär kostnadsökningar och intäktsminskningar för det allmänna, dvs. staten, kommuner eller landsting, åligger det utredningen att i sådant fall också föreslå en finansiering.

Våra förslag innebär i huvudsak ett införande av dels två nya straffprocessuella tvångsmedel, dels en särskild straffskala för grovt dataintrång. De förslag som vi redovisar bedöms kunna få vissa ekonomiska konsekvenser för staten och vissa företag samt ha viss, om än marginell, betydelse för brottsligheten och det brottsförebyggande arbetet. I övrigt har förslagen ingen betydelse för de många övriga angivna intressen, vilka enligt kommittéförordningen ska beaktas i utredningssammanhang. Det föreläggande att under viss tid bevara lagrade elektroniska uppgifter som vi föreslår ska visserligen även kunna riktas mot enskilda men föreläggande kommer enligt vår uppfattning i praktiken inte att användas mot enskilda personer. I dessa

fall kommer de brottsutredande myndigheterna även i framtiden att använda sig av husrannsakan och beslag för att säkra elektroniska uppgifter.

De ekonomiska effekterna, liksom betydelsen för brottsprevention redovisas i följande avsnitt.

10.2 Ekonomiska konsekvenser

10.2.1 Konsekvenser för staten

Bedömning: Våra förslag kan komma att leda till vissa kostnadsökningar för rättsväsendet men innebär samtidigt att resursutnyttjandet i rättsväsendet kan bli något effektivare. Kostnadsökningarna inom rättsväsendet är inte sådana att de måste finansieras i särskild ordning.

Förslagen kan komma att leda till ökade kostnader för Post- och telestyrelsen. De kan dock inte förväntas få annat än en högst marginell påverkan på myndighetens kostnader.

Skälen för bedömningen

De kostnader som kan beräknas uppkomma för staten till följd av våra förslag kan mer eller mindre uteslutande hänföras till rättsväsendet.

Vi har lämnat förslag till två nya straffprocessuella tvångsmedel: bevarandeföreläggande och föreläggande att lämna upplysningar i syfte att underlätta husrannsakan i it-miljö. Det första innebär att någon som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott ska kunna föreläggas att bevara uppgiften under viss tid. Att det införs en möjlighet att ge ett bevarandeföreläggande innebär att elektroniska uppgifter som i dag går förlorade innan de brottsutredande myndigheterna hunnit säkra dem genom de medel som för närvarande står till buds (husrannsakan och beslag, edition och hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation) i framtiden i vissa situationer kommer att kunna bevaras och användas i brottsutredningar. Bevarandeföreläggande är ett enkelt, snabbt och smidigt sätt att säkra elektroniska uppgifter.

Det andra tvångsmedlet innebär att den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där ska kunna föreläggas att lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Syftet är således att underlätta husrannsakan i it-miljö. Det kan förväntas att möjligheten att ge föreläggande att lämna upplysningar kommer att innebära att husrannsakan i it-miljö i större utsträckning än i dag leder till resultat och att sådana uppgifter som den brottsutredande myndigheten söker efter kan säkras innan de förstörs eller ändras.

Sammanfattningsvis torde våra ändringsförslag i dessa delar bidra till en mer effektiv bekämpning av såväl brottslighet som är direkt it-relaterad som annan brottslighet där det finns bevisning i elektronisk form. Fler brottsutredningar kommer sannolikt att leda till åtal och lagföring.

Att fler brottsutredningar leder till åtal kommer att innebära ökade kostnader för framför allt polis-, åklagar- och domstolsväsendet. Den nya lagstiftningen kommer också att medföra att det i ett inledningsskede kommer att uppstå kostnader för information, utbildning och ändringar i handböcker, informationsmaterial och liknande. Samtidigt måste vägas in att vissa effektivitetsvinster för rättsväsendet torde uppstå genom förslagen eftersom det blir enklare och snabbare både att få tillgång till elektronisk bevisning vid en husrannsakan genom föreläggande att lämna upplysningar och att säkra viss elektronisk bevisning genom bevarandeföreläggande.

Enligt våra förslag ska den som ålagts ett bevarandeföreläggande få begära rättens prövning av det och om den som förelagts att lämna upplysningar som behövs för att en husrannsakan i it-miljö ska kunna verkställas vägrar att göra detta, ska vittnesförhör med honom eller henne kunna äga rum inför rätten. Detta kan leda till en i viss mån ökad belastning på domstolsväsendet. Hur stor den ökade belastningen blir beror dock på hur ofta beslut om bevarandeföreläggande och föreläggande att lämna upplysningar kommer att fattas och hur stor andel av dessa som kommer att kräva rättens medverkan. Det är svårt att med någon säkerhet uppskatta hur många beslut om de två nya formerna av föreläggande som kommer att fattas. Enligt en nyligen framtagen utvärderingsrapport av den kommitté inom Europarådet som övervakar konventionen (the Cybercrime Convention Committee [T-CY]) har, i de länder som tillträtt konventionen och infört en möjlighet till föreläggande motsvarande den som vi föreslår, denna åtgärd, med undantag för USA, inte använts

så frekvent i nationella brottsutredningar. I nationella brottsutredningar har i stället andra medel för säkrande, såsom husrannsakan och beslag, använts (Assessment report, *Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, Version 14 November 2012, s. 10). Vid begäran om rättslig hjälp med säkrande av elektroniska uppgifter från en annan stat har åtgärden dock använts mer frekvent. Oavsett hur många förelägganden som kommer att beslutas uppskattar vi emellertid att bevarandeföreläggande ytterst sällan kommer att behöva underställas rättens prövning och att det även kommer att vara ytterst sällan som den som meddelat ett föreläggande att lämna upplysningar kommer att behöva gå vidare och begära vittnesförhör inför rätta med den som förelagts. Förslagen om bevarandeföreläggande och föreläggande att lämna upplysningar kan därför inte beräknas få annat än en begränsad påverkan på arbetsbördan för domstolarna.

Som vi tidigare angett kan det förutspås att de nya straffprocessuella tvångsmedel som vi föreslår kommer att leda till ett ökat antal lagföringar. I den mån de resulterar i annan påföljd än böter kan det komma att innebära ökade kostnader för Kriminalvården. Förslaget om en särskild straffskala för grovt dataintrång kan få samma konsekvens. Det är dock svårt att uppskatta i vilken utsträckning lagföringarna kommer att öka, i vilken mån de kommer att leda till fängelse- eller frivårdspåföljder och i vilken utsträckning den särskilda straffskalan för grovt dataintrång kommer att utnyttjas. Det är därför inte möjligt att med någon större tillförlitlighet beräkna vilka kostnader som kommer att uppstå för Kriminalvården och när i tid de kommer att uppstå. Vi gör dock bedömningen att de ekonomiska konsekvenserna för Kriminalvårdens del inte blir mer omfattande än att de ryms inom nuvarande budgetramar.

Vi har gjort bedömningen att kravet i konventionens artikel 35 på en kontaktpunkt som alltid är tillgänglig kan uppfyllas genom utseende av Rikspolisstyrelsen som kontaktpunkt och att Sverige bör lämna underrättelse om att Rikspolisstyrelsen ska vara kontaktpunkt för utbytet av uppgifter enligt direktivets artikel 14. Mot bakgrund av det åtagande som i detta avseende följer av konventionen och direktivet kan det krävas en översyn av resursfördelningen inom Rikspolisstyrelsen så att den enhet som i praktiken ska fungera som kontaktpunkt förfogar över de resurser som krävs för att fullgöra denna uppgift. Uppgiften är dock enligt vår bedömning inte mer betungande än att den ryms inom myndighetens nuvarande budgetramar.

Sammantaget är det vår bedömning att genomförandet av våra förslag inte kommer att leda till mer än begränsade kostnadsökningar för polismyndigheterna, åklagarväsendet, domstolsväsendet och Kriminalvården. Dessa ökningar bör kunna finansieras inom ramen för befintliga anslag hos de berörda myndigheterna.

Den myndighet som utöver rättsväsendet kan komma att få ökade kostnader till följd av våra förslag är Post- och telestyrelsen (PTS). Vi har föreslagit att PTS, på samma sätt som när det gäller de trafikuppgifter som lagrats för brottsbekämpande syften enligt 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation (LEK), ska utöva tillsyn över operatörernas skyldighet att bevara uppgifter enligt den föreslagna bestämmelsen i rättegångsbalken. Vi har vidare föreslagit att PTS, på samma sätt som när det gäller ersättning för kostnader som uppstår när uppgifter som lagrats enligt 6 kap. 16 a § LEK lämnas ut, ska meddela föreskrifter om ersättning i samband med att uppgifter som bevarats enligt rättegångsbalken lämnas ut. PTS har i uppdrag att utöva tillsyn enligt LEK och i uppdraget ingår specifikt att utföra nu angivna uppgifter när det gäller lagring av trafikuppgifter. Även om myndigheten kommer att behöva lägga ner vissa resurser på att åstadkomma en effektiv tillsyn över leverantörernas hantering även av uppgifter som ska bevaras och en ordning för ersättning vid utlämnande av uppgifter som ska bevaras, finns en upparbetad kompetens inom myndigheten för frågorna. I samband med att PTS fick uppdraget att utöva tillsyn över leverantörernas lagring av trafikuppgifter gjorde myndigheten bedömningen att verksamheten behövde tillföras ca 3 miljoner kronor det första året, ca 2 miljoner kronor det andra året och därefter knappt en miljon kronor årligen. Regeringen gjorde i det sammanhanget bedömningen att PTS utökade verksamhet på området skulle finansieras genom ökade avgifter och att det fick ankomma på PTS att täcka de ökade kostnaderna genom avgifter (prop. 2010/11:46 s. 71). Vi gör bedömningen att de ekonomiska konsekvenserna av våra förslag för PTS del blir tämligen marginella och att några ytterligare medel inte kommer att behöva tillföras myndigheten.

För Brottförebyggande rådet (Brå) kan förslaget om en särskild straffskala för grovt dataintrång tänkas medföra en viss, om än ytterst marginell, merkostnad eftersom en ny brottskod för grovt dataintrång kommer att behöva införas.[1]

[1] Att koda brott innebär att bestämma dels brottskod (sifferbeteckning enligt kodlistan), dels brottsantal för de brottsliga gärningar som vid anmälansupptagningen ska registreras i polisens, åklagarväsendets, ekobrottsmyndighetens och tullens datasystem för registrering av

10.2.2 Konsekvenser för företag

Bedömning: Införandet av en möjlighet att förelägga den som i elektronisk form innehar en viss lagrad uppgift att bevara uppgiften under viss tid kan komma att medföra vissa kostnader för företag mot vilka föreläggande riktas. Detsamma gäller införandet av en möjlighet att ge föreläggande att lämna upplysningar i syfte att underlätta en husrannsakan it-miljö. Vi bedömer dock att våra förslag sammantaget inte kommer att få annat än en högst marginell påverkan på berörda företags kostnader.

Skälen för bedömningen

Vårt förslag om bevarandeföreläggande innebär att det ska vara möjligt att förelägga den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften under viss tid, högst 90 dagar med möjlighet till högst 30 dagars förlängning, om det finns särskilda skäl för det. Ett bevarandeföreläggande ska kunna riktas mot såväl fysiska som juridiska personer och mot leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Ett införande av en möjlighet till bevarandeföreläggande i den form som vi föreslår utgör enligt vår bedömning en förutsättning för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll.

Om ett bevarandeföreläggande riktas mot ett företag – exempelvis det företag på vilket en misstänkt person arbetar eller en operatör enligt LEK – kan det givetvis komma att innebära vissa kostnader för företaget. Vårt förslag är emellertid utformat så att föreläggande ska avse ”en viss lagrad uppgift”, vilket innebär dels att uppgiften redan måste finnas lagrad och sparad hos den som föreläggandet riktar sig mot, dels att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras. Föreläggandet kan således varken innebära att uppgifter som inte redan är lagrade ska bevaras eller komma att gälla hela servrar hos företag. Föreläggandet kan tänkas bli uppfyllt på olika sätt. Ett alternativ är att den som föreläggandet riktar sig mot kopierar uppgiften. Ett

anmälningar och misstankar. Kodningen ligger till grund för Sveriges officiella statistik men också för polisens operativa verksamhet, resultatredovisning och resursfördelning (se Brå:s publikation *Kodning av brott, Anvisningar och regler*, Version 11.0, s. 7).

annat är att uppgiften lämnas orubbad på sin ursprungliga plats, samtidigt som åtgärder vidtas så att den inte kan raderas eller ändras på något sätt. Vid behov får den som har beslutat om föreläggandet, eventuellt i samråd med den som föreläggandet riktar sig mot, ge anvisningar om hur uppgiften bör bevaras i det enskilda fallet för att bevarandeskyldigheten ska anses ha blivit uppfylld.

Som tidigare nämnts är det svårt att med någon säkerhet uppskatta hur många beslut om bevarandeföreläggande som kommer att fattas. Den utvärderingsrapport från Europarådet som vi nämnt i avsnitt 10.2.1 visar på att åtgärden inte använts särskilt ofta i nationella förundersökningar i de stater som infört en möjlighet till föreläggande i sin nationella lagstiftning.

Mot bakgrund av vad som anförts är det vår uppfattning att förslaget om bevarandeföreläggande generellt sett kommer att få en högst marginell påverkan på berörda företags kostnader.

När det mer specifikt gäller de operatörer som omfattas av regleringen i LEK kan följande sägas. Om ett bevarandeföreläggande riktas mot någon som är anmälningspliktig enligt 2 kap. 1 § LEK har vi föreslagit att bestämmelserna i 6 kap. LEK om rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut (16 e §) och om anpassning för utlämnande av uppgifter (16 f §)ska gälla även för uppgifter som omfattas av ett bevarandeföreläggande. Operatören kommer således att få ersättning för bevarandet vid utlämnandet av den myndighet som har begärt uppgifterna enligt föreskrifter som meddelas av PTS.

När det gäller den skyldighet att lämna ut uppgifter om vilka övriga leverantörer som har som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande som vi föreslår, innebär inte heller förslaget i denna del något nytt krav på att spara uppgifter. Informationen ska enbart lämnas ut om det är möjligt för leverantören att få fram den ur uppgifter som redan finns lagrade. Detta innebär givetvis att viss arbetstid måste läggas på att ta fram informationen och att kommunicera den med den myndighet som begär att få den. Vi bedömer dock att detta inte kan vara särskilt betungande. Uppgifter om vilka övriga leverantörer är som deltagit vid överföringen av ett meddelande kommer vidare enligt vår uppfattning i den övervägande delen av fallen att kunna fås fram genom de trafikuppgifter som lagras enligt 6 kap. 16 a § LEK. Leverantörerna kommer då, enligt 6 kap. 16 e § LEK, ha rätt till ersättning för kostnader som uppstår i samband med att uppgift om vilka övriga leverantörer är lämnas ut.

Vad avser vårt förslag om en möjlighet att förelägga den som kan antas ha upplysningar som behövs för att ett beslut om husrannsakan i it-miljö ska kunna verkställas att lämna ut upplysningarna, kan det innebära att det företag hos vilket husrannsakan vidtas får ställa viss arbetskraft till förfogande under det att ett visst datasystem genomsöks. Det är emellertid inte fråga om något större engagemang i sammanhanget utan handlar enbart om att lämna ut lösenord, åtkomstkoder etc. eller att beskriva det datasystem som ska genomsökas. Vi anser inte att vårt förslag i denna del kommer att innebära större kostnader för företag än de som företag redan i dag får vidkännas i samband med att husrannsakan företas i deras lokaler. Snarare kan kostnaderna bli mindre eftersom en husrannsakan, om de brottsutredande myndigheterna får tillgång till den information som behövs för att datasystemet och uppgifterna däri ska kunna genomsökas och granskas, kan genomföras på ett smidigare och snabbare sätt och företaget därför får vidkännas mindre avbräck i sin verksamhet.

10.3 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Bedömning: Våra förslag kan antas medföra vissa positiva effekter framför allt för det brottsförebyggande arbetet.

Skälen för bedömningen

När det gäller våra förslag på straffprocessrättens område utgör i vart fall förslaget om bevarandeföreläggande en förutsättning för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll. Ett tillträde till konventionen och tilläggsprotokollet kommer att underlätta Sveriges möjligheter att bistå andra stater med rättslig hjälp på området för it-relaterad brottslighet och att aktivt delta i det internationellt brottsförebyggande och brottsbekämpande arbetet. Att Sverige kan bistå andra stater med rättslig hjälp när det gäller exempelvis skyndsamt säkrande av lagrade elektroniska uppgifter kan även få allmänna positiva effekter på det nationellt brottsbekämpande planet, genom

att andra stater i större utsträckning går Sverige till mötes, när Sverige begär rättslig hjälp på området för it-relaterad brottslighet.

När det gäller förslaget om en särskild straffskala för grovt dataintrång är det naturligtvis osäkert vilken direkt inverkan detta får på brottsligheten. Detta gäller särskilt som personuppklaringsprocenten för dataintrång hittills varit mycket låg. En särskild straffskala för grovt dataintrång bör dock kunna ge vissa brottsförebyggande effekter. Den skärpta synen visar på en betydligt allvarligare inställning från samhällets sida på framför allt allvarliga former av illegala dataangrepp. Detta bör ge en signal till myndigheter och andra aktörer i samhället att prioritera åtgärder som syftar till att förebygga och bekämpa sådan brottslighet. Samtidigt bör man notera att det är svårt att hänföra eventuella effekter av detta slag till en specifik lagändring, eftersom det även kan finnas andra förändringar i samhället som kan påverka brottsutvecklingen.

11 Ikraftträdande och övergångsbestämmelser

11.1 Ikraftträdande

Förslag: De föreslagna lagändringarna ska träda i kraft den 1 januari 2015.

Skälen för förslaget

De lagändringar som vi har föreslagit bör träda i kraft så snart som möjligt för att möjliggöra ett svenskt tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll. Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet, inhämtande av Lagrådets yttrande och riksdagsbehandling bör de nya bestämmelserna kunna träda i kraft den 1 januari 2015.

Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF är ännu inte (per den 20 maj 2013) formellt antaget. Efter att direktivet antas har medlemsstaterna två år på sig att genomföra det. Om vårt förslag om en särskild straffskala för grovt dataintrång träder i kraft den 1 januari 2015 innebär det att Sverige med god marginal kommer att ha genomfört direktivet inom den föreskrivna tiden.

11.2 Övergångsbestämmelser

Bedömning: De föreslagna lagändringarna kräver inte några särskilda övergångsbestämmelser.

Skälen för bedömningen

Enligt allmänna principer får ny lag inte retroaktiv verkan. Beträffande strafflagstiftning är detta lagfäst i 2 kap. 10 § regeringsformen och artikel 7 i Europakonventionen, vilken gäller som svensk lag.

Enligt 2 kap. 10 § regeringsformen får således straff eller annan brottspåföljd inte åläggas för gärning som inte var belagd med brottspåföljd när den förövades. Inte heller får någon dömas till svårare brottspåföljd för gärningen än den som var föreskriven då. En bestämmelse om förbud mot retroaktiv strafflagtillämpning finns även i 5 § lagen (1964:163) om införande av brottsbalken.

Att den särskilda straffskala för grovt dataintrång som vi föreslår ska tillämpas endast i fråga om gärningar som begås efter ikraftträdandet följer således av såväl allmänna principer som de lagrum som redovisats. Det behövs följaktligen inte någon särskild övergångsbestämmelse om detta.

När det gäller processrättslig lagstiftning är utgångspunkten att nya regler ska tillämpas genast efter ikraftträdandet. Det innebär att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. De processrättsliga lagändringar vi föreslår, t.ex. gällande bevarandeföreläggande och föreläggande att lämna upplysningar inom ramen för en husrannsakan i it-miljö, kommer i enlighet med huvudprincipen att tillämpas från och med att de träder i kraft och då även i förundersökningar som har inletts innan de föreslagna bestämmelserna träder i kraft. Vi bedömer därför att det inte heller i övrigt behövs några övergångsbestämmelser.

12 Författningskommentar

12.1 Förslaget till lag om ändring i rättegångsbalken

27 kap.

16 § *Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott får föreläggas att bevara uppgiften.*

I föreläggandet ska anges under hur lång tid uppgiften ska bevaras. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga 90 dagar. Om det finns särskilda skäl får tiden för bevarande förlängas med högst 30 dagar.

Föreläggande får inte riktas mot den som skäligen kan misstänkas för brottet eller någon honom eller henne sådan närstående person som avses i 36 kap. 3 §.

Paragrafen är ny. Den innehåller bestämmelser som gör det möjligt för brottsutredande myndigheter att i en brottsutredning skyndsamt säkra lagrade elektroniska uppgifter som kan antas ha betydelse för utredningen. Syftet är att de elektroniska uppgifterna ska bevaras och behållas intakta under viss tid, i avvaktan på att de brottsutredande myndigheterna vidtar åtgärder för att få tillgång till uppgifterna, dvs. tar bevisningen i beslag, begär editionsföreläggande eller begär tillstånd till hemlig övervakning eller hemlig avlyssning av elektronisk kommunikation. De allmänna övervägandena finns i avsnitt 8.3.2.

Första stycket innebär att den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott får föreläggas att bevara uppgiften. De elektroniska uppgifter som ett föreläggande kan avse kan vara av vilket slag som helst. Det kan således exempelvis röra sig om att bevara en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat. En begränsning ligger i att uppgiften måste finnas lagrad redan då föreläggandet meddelas.

Någon kan alltså inte föreläggas att framöver lagra eller spara uppgifter. Att uppgiften är lagrad betyder att den ska finnas bevarad elektroniskt.

Ytterligare en begränsning ligger i att föreläggandet ska avse ”en viss” elektronisk uppgift. I föreläggandet måste således anges vilken specifik elektronisk uppgift som ska bevaras, exempelvis en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan alltså inte tillåtas vara generellt i den meningen att den som föreläggandet riktar sig mot exempelvis ska bevara alla uppgifter som mottagits under en viss tidsperiod.

Föreläggandet kan rikta sig mot vem som helst som innehar de lagrade elektroniska uppgifterna. Det kan alltså riktas mot såväl fysiska som juridiska personer, inklusive leverantörer av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Undantag finns dock enligt tredje stycket för misstänkta och till den misstänkte närstående personer. De lagrade uppgifterna ska antingen finnas hos personen eller på annat sätt finnas under personens kontroll och åtkomst. En lagrad uppgift kan innehas av olika personer och aktörer samtidigt, exempelvis om en person har olika dokument eller sin e-post lagrad på en server någon annanstans än där han eller hon befinner sig. Ett bevarandeföreläggande kan då rikta sig såväl mot den som på distans har kontroll över och åtkomst till de elektroniska uppgifterna som mot den som innehar servern.

När elektroniska uppgifter lagras på en server på distans är det ofta slumpmässigt var någonstans servern befinner sig. Den enskilde är heller inte sällan själv ovetande om på vilken plats servern står som uppgifterna har lagrats på. Mot den bakgrunden bör den som utfärdar ett bevarandeföreläggande inte redan i samband med att föreläggandet meddelas behöva ta reda på var de elektroniska uppgifterna finns lagrade, så länge den som föreläggandet riktar sig mot befinner sig i Sverige och har åtkomst till och kontroll över uppgifterna härifrån. En annan sak är att de brottsutredande myndigheterna i fall där uppgifterna finns lagrade på en server utomlands inte får använda sig av möjligheten till bevarandeföreläggande i syfte att kringgå de bestämmelser om rättslig hjälp som reglerar frågan om utlämnande av uppgifterna.

Något krav på att förundersökningen har kommit så långt att någon är skäligen misstänkt för brottet finns inte. Det är tillräckligt att någon innehar viss lagrad i uppgift i elektronisk form som skäligen kan antas ha betydelse för utredningen om ett brott. Något krav på

det aktuella brottets svårhetsgrad finns inte heller. Av proportionalitetsprincipen följer dock att de brottsbekämpande myndigheterna inte ska meddela ett bevarandeföreläggande om de redan då de överväger att meddela föreläggandet kan se att det, mot bakgrund av brottets svårhet eller av andra skäl, inte finns någon möjlighet att med stöd av de regler som gäller för detta, senare få ut de uppgifter som skulle säkras.

Ett föreläggande om bevarande kan tänkas bli uppfyllt på olika sätt. Ett alternativ är att den som föreläggandet riktar sig mot kopierar uppgiften. Ett annat är att uppgiften lämnas orubbad på sin ursprungliga plats, samtidigt som åtgärder vidtas så att den inte kan raderas eller ändras på något sätt. Vid behov får den som har beslutat om föreläggandet, eventuellt i samråd med den som föreläggandet riktar sig mot, ge anvisningar om hur uppgiften bör bevaras i det enskilda fallet för att bevarandeskyldigheten ska anses ha blivit uppfylld.

Av *andra stycket* framgår att det i föreläggandet ska anges under hur lång tid uppgiften ska bevaras. Vidare framgår att tiden för bevarande aldrig får vara längre än vad som är nödvändigt i det enskilda fallet och att bevarandetiden då föreläggandet meddelas aldrig får sättas till längre tid än 90 dagar. En möjlighet att förlänga den ursprungliga tiden för bevarande med högst 30 dagar finns dock om det finns särskilda skäl för det. Särskilda skäl kan exempelvis finnas om en begäran om säkrande av elektroniska uppgifter kommit in från en annan stat och den svenske åklagaren måste sätta sig in i viss utländsk lagstiftning i samband med en efterföljande begäran om utlämnande av uppgifterna. Uppgifterna måste då kunna hållas fortsatt bevarade i avvaktan på prövning av frågan om de går att lämnas ut enligt de regler som gäller för detta. Även i vissa mer komplicerade svenska utredningar kan tänkas att det kan finnas särskilda skäl att förlänga bevarandetiden.

Tredje stycket innehåller ett förbud mot att rikta ett bevarandeföreläggande mot den som skäligen kan misstänkas för det brott som utreds, i de fall utredningen har kommit så långt att någon är misstänkt. Föreläggande får i de fallen inte heller riktas mot någon den misstänkte sådan närstående person som avses i 36 kap. 3 §.

Den som låter bli att följa ett bevarandeföreläggande kan i vissa situationer, exempelvis vid uppsåtlig radering av de uppgifter som omfattas av föreläggandet, hållas straffrättsligt ansvarig enligt bestämmelsen om överträdelse av myndighets bud i 17 kap. 13 § brottsbalken.

16 a § *Föreläggande enligt 16 § beslutas av undersökningsledaren eller åklagaren. Om det är möjligt ska föreläggandet ges skriftligt. I annat fall ska den förelagde så snart som möjligt få ett skriftligt bevis om beslutet.*

Meddelande om åtgärden får inte obehörigen föras vidare. Föreläggandet ska innehålla en underrättelse om detta.

Den som ålagts föreläggandet får begära rättens prövning av föreläggandet. För rättens prövning gäller i tillämpliga delar vad som sägs i 6 §.

Paragrafen är ny. De allmänna övervägandena finns i avsnitt 8.3.2.

I *första stycket* regleras först vem som får besluta om att utfärda ett bevarandeföreläggande enligt 16 §. Beslutsbefogenheten tillkommer undersökningsledaren eller åklagaren. I vissa fall kommer även Tullverket, med stöd av 19 § lagen (2000:1225) om straff för smuggling, kunna besluta om bevarandeföreläggande. I stycket anges vidare att ett bevarandeföreläggande som huvudregel ska vara skriftligt. Föreläggandets omfattning ska tydligt framgå av beslutet. Om det inte är möjligt att ge ett skriftligt föreläggande, vilket exempelvis kan vara fallet om ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande, får föreläggandet ges muntligen. Den förelagde ska då emellertid så snart som möjligt få ett skriftligt bevis om beslutet.

Av *andra stycket* framgår att den som förelagts att bevara uppgifterna är skyldig att hemlighålla att säkrande åtgärder har vidtagits och att föreläggandet ska innehålla en underrättelse om detta. För den som utan tillstånd bryter mot skyldigheten att hemlighålla att säkringsåtgärder vidtagits kan straffansvar utkrävas enligt 9 kap. 6 §. För tystnadspliktens omfattning i de fall då rätten enligt tredje stycket prövat ett bevarandeföreläggande hänvisas till de allmänna övervägandena.

Enligt *tredje stycket* får den som ålagts ett bevarandeföreläggande begära rättens prövning av det. Ett bevarandeföreläggande gäller dock fram till dess att rätten eller den som ursprungligen har meddelat föreläggandet meddelar något annat. Mot bakgrund av att det finns möjlighet att begära rättens prövning bör föreläggandet innehålla en uppgift om vilken domstol som i förekommande fall ska pröva frågan. För rättens prövning gäller de regler som gäller för prövning av beslag. Om den som ålagts ett föreläggande begär rättens prövning av föreläggandet, ska rätten därmed hålla förhandling så snart som möjligt och, om det inte finns något synnerligt hinder mot det, senast fjärde dagen efter det att begäran om prövning har kommit in. Frågan om bevarandeföreläggandet ska bestå är en sak

mellan den som ålagts föreläggandet och den som beslutat det. Om det finns en misstänkt person har han eller hon alltså inte någon rätt att närvara vid förhandlingen och ska inte underrättas om eller kallas till denna. Rättens beslut kan överklagas av någon av parterna med stöd av 49 kap. 5 § 6. Om rätten upphäver föreläggandet kan undersökningsledaren eller åklagaren enligt 52 kap. 7 § tredje stycket begära inhibition, i syfte att förhindra att bevisningen går förlorad innan överinstansen har hunnit ta ställning i frågan.

28 kap.

7 a § *Undersökningsledaren eller åklagaren får förelägga den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där att lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Beslut om föreläggande ska dokumenteras.*

Om någon skäligen kan misstänkas för brottet får föreläggande inte riktas mot den misstänkte. Föreläggande får inte heller riktas mot den som, om åtal väcks, inte skulle vara skyldig att vittna i målet om omständighet som avses i första stycket.

Vägrar den förelagde att lämna upplysningar får på undersökningsledarens eller åklagarens begäran vittnesförhör med honom eller henne äga rum inför rätten. Om förhöret gäller i tillämpliga delar vad som föreskrivs om bevisupptagning utom huvudförhandling. En misstänkt får beredas tillfälle att närvara vid förhöret om det kan ske utan men för utredningen.

Paragrafen är ny. Den innehåller bestämmelser som gör det möjligt att utfärda föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö. De allmänna övervägandena finns i avsnitt 8.3.4.

Enligt *första stycket* får den som kan antas känna till funktionerna i eller andra förutsättningar för åtkomst till ett visst datasystem och granskning av uppgifterna där föreläggas att lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Föreläggande kan alltså riktas mot systemadministratörer eller andra personer som har kunskap om det datasystem som ska genomsökas. Det ska finnas konkreta omständigheter som pekar på att den person som föreläggs känner till det datasystem som de brottsutredande myndigheterna vill genomsöka.

Ett föreläggande innebär att personen ska lämna de upplysningar som behövs för att ett beslut om husrannsakan ska kunna verkställas. Vilka upplysningar som behövs är beroende av omständig-

heterna i det enskilda fallet. Det kan röra sig om att beskriva det datasystem som ska undersökas eller att uppge lösenord och åtkomstkoder. Det kan också handla om att lämna dekrypteringsnycklar eller att ange var föremål som bär dessa nycklar finns så att de uppgifter som finns i systemet kan läsas eller att ange vilken av ett flertal servrar som den information som de brottsutredande myndigheterna vill genomsöka finns lagrad på.

För att föreläggande ska få meddelas ställs inte upp något krav på att utredningen har kommit så långt att någon är skäligen misstänkt för det brott som utreds.

Beslutsbefogenheten att utfärda föreläggande tillkommer undersökningsledaren eller åklagaren. Även Tullverket kan, med stöd av 19 § lagen (2000:1225) om straff för smuggling, utfärda föreläggande. Ett beslut att utfärda föreläggande ska dokumenteras på lämpligt sätt.

Av *andra stycket* framgår att, för det fall utredningen har kommit så långt att någon skäligen kan misstänkas för det brott som föranlett husrannsakan, föreläggande inte får riktas mot den misstänkte. Vidare framgår att även vissa andra personer är undantagna från upplysningsplikten. Föreläggande får inte riktas mot den som, om åtal väcks, inte skulle vara skyldig att vittna i målet. Inte heller får föreläggande riktas mot den som visserligen skulle vara skyldig att vittna i målet men inte skulle få höras som vittne om sådan uppgift som de brottsutredande myndigheterna vill få tillgång till. Föreläggande att lämna upplysningar kan således exempelvis inte riktas mot den misstänktes närstående eller mot hans eller hennes försvarare, om denne har fått del av sin klients lösenord vid fullgörande av sitt uppdrag.

I *tredje stycket* anges den möjlighet till sanktion mot den som förelagts att lämna upplysningar men vägrar att göra detta som står till buds. Undersökningsledaren eller åklagaren får då begära att vittnesförhör med honom eller henne äger rum inför rätten. Om förhöret gäller i tillämpliga delar vad som föreskrivs om bevisupptagning utom huvudförhandling. För det fall den förelagde även inför rätten skulle vägra att lämna upplysningar kan rätten, med stöd av 36 kap. 21 §, förelägga honom eller henne vid vite, och om det inte skulle vara verksamt, vid äventyr av häkte att lämna upplysningarna. Till skillnad från vad som gäller enligt bestämmelserna i 23 kap. 13 § om vittnesförhör inför rätta under en förundersökning krävs inte att någon skäligen kan misstänkas för brottet och även om det finns en skäligen misstänkt får han eller hon ges till-

fälle att närvara vid förhöret endast om det kan ske utan men för utredningen.

12.2 Förslaget till lag om ändring i brottsbalken

4 kap.

9 c § Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för *dataintrång* till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

Om brottet är grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art.

Paragrafen innehåller bestämmelser om straff för dataintrång. De allmänna övervägandena finns i avsnitt 9.4.

I *första stycket* är den enda ändringen att dataintrångsbestämmelsen inte längre ska vara subsidiär till bestämmelserna om brytande av post- eller telehemlighet (4 kap. 8 § brottsbalken) och om intrång i förvar (4 kap. 9 § brottsbalken). Förhållandet mellan dataintrång och övriga brottsbalksbrott får i fortsättningen avgöras enligt sedvanliga principer för bedömningen av konkurrens mellan överlappande straffstadganden i brottsbalken, se närmare i det följande.

I *andra stycket*, som är nytt, införs en särskild straffskala för grovt dataintrång.

Vid bedömande av om brottet är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art. Uppräkningen är inte uttömmande. Även andra omständigheter kan beaktas. Domstolen ska göra en helhetsbedömning av samtliga omständigheter i det enskilda fallet.

För att kunna fungera på det sätt som medborgarna generellt förväntar sig är samhället beroende av fungerande datasystem. Såväl drifts- och säkerhetsrelaterad information som uppgifter om enskilda personer och företag behandlas och lagras elektroniskt. Enskilda,

myndigheter och företag ställer krav på säkra och välfungerande datasystem. Samhällets beroende av datasystemen gör också att angrepp mot systemen kan orsaka betydande ekonomiska skador i form av avbrott eller kostnader för att återställa driften. Samtidigt är det intresse som ligger bakom kriminaliseringen av manipulationer av elektroniskt baserade uppgifter och processer inte begränsad till de rent ekonomiska faktorerna. Det finns också ett starkt intresse av att skydda säkerheten i systemen och allmänhetens tillit till dem. På det sättet finns likheter med förfalskningsbrotten. Skyddsintresset är således vidsträckt.

Med begreppet allvarlig skada avses bl.a. störningar av viktiga samhällsfunktioner. Som exempel på sådana kan anges uppgifter i polisens eller Försvarsmaktens datasystem. Men det behöver inte vara fråga om myndigheters verksamheter. Många viktiga samhällsfunktioner upprätthålls av privata aktörer, t.ex. finansiella system, olika processer för industriell verksamhet eller annan liknande informationsbehandling. Allvarlig skada i bestämmelsens mening kan uppkomma även i verksamhet som inte kan sägas upprätthålla några direkt viktiga samhällsfunktioner. Ett angrepp mot ett företag som enbart drivs av kommersiella intressen för privat vinnings skull och där skadan endast är av ekonomisk natur kan anses som grovt dataintrång om den ekonomiska skadan är betydande.

Vid bedömningen av om en verksamhet har orsakats allvarlig skada i den mening som avses i bestämmelsen ska vid sidan av de rent ekonomiska effekterna, vilka inbegriper kostnader för nedlagt arbete och för att få systemet att fungera, beaktas även de skadeverkningar i övrigt som ett rubbat förtroende har fört med sig.

Motsvarande bedömning får göras i de fall gärningen i första hand riktas mot enskildas personliga integritet. Allvarlig ideell skada skulle kunna uppkomma vid intrång i exempelvis datasystem med patientjournaler. Förlust eller förvanskning av hemlig eller i övrigt integritetskänslig information kan således innebära att allvarlig skada uppkommit i bestämmelsens mening. Om ingrepp har skett i ett system med särskilt integritetskänslig information kan det även leda till att det anses nödvändigt att byta ut systemet, vilket i sig kan få stora ekonomiska följder. Till denna kategori kan höra fall av identitetsstöld som får långtgående och allvarliga konsekvenser för den enskilde.

Omständigheten att gärningen har avsett ett stort antal uppgifter tar bl.a. sikte på omfattande tillgänglighets- eller överbelastningsattacker som inneburit allvarliga ingrepp i viktiga kommunika-

tioner. Som framhållits i de allmänna övervägandena kan sådana attacker, mot bakgrund av den stora betydelse som informationssystem har i dagens samhälle, även om de ekonomiska skadorna av dem kan vara svåra att uppskatta, få allvarliga konsekvenser och orsaka svåra störningar på viktiga samhällsfunktioner. Även andra typer av attacker täcks in av omständigheten om en betydande mängd uppgifter har påverkats på något av de sätt som nämns i första stycket, exempelvis då ett stort antal uppgifter har raderats eller ändrats. Detsamma gäller om någon olovligen berett sig tillgång till en stor mängd uppgifter.

Omständigheten att gärningen varit av särskilt farlig art innebär att själva tillvägagångssättet vid gärningen eller det mål som den riktar sig mot ensamt kan kvalificera brottet som grovt. Av särskilt farligt art kan attacker vara som kunnat få mycket allvarliga konsekvenser. Attacker eller intrång i bankers informationssystem med risk för att förtroendet för bankväsendet och betalningssystemet raseras hör till denna kategori. I vissa fall kan det alltså anses vara lika farligt att genom en attack av något slag skapa en osäkerhet om ett systems tillförlitlighet som att orsaka reella skador på systemet. En skapad osäkerhet om huruvida ett visst system går att lita på och som i förlängningen kan leda till en brist i tilliten till säkerheten i samhällsviktig infrastruktur kan få vittgående konsekvenser såväl för den enskilde som för företag, myndigheter och samhället i stort.

Frågan om ett dataintrång ska bedömas som grovt ska avgöras med beaktande av samtliga omständigheter vid brottet. Ett brott kan bedömas som grovt även om inte någon av de uppräknade omständigheterna har förelegat. Samtidigt innebär inte förekomsten av en av de uppräknade omständigheterna att brottet alltid ska bedömas som grovt.

Minimistraffet för grovt dataintrång är sex månaders fängelse och straffmaximum sex års fängelse. Inom straffbudet ryms gärningar av skiftande karaktär. Som framgått förutsätts en betydande kvalificering för att gärningen ska anses ha ett straffvärde enligt den nya bestämmelsen. Straffvärdet bestäms av gärningens allvar vilket bedöms utifrån den skada, kränkning och fara som gärningen har inneburit. Samtliga omständigheter i det enskilda fallet ska beaktas vid straffvärdebedömningen. De kriterier som är avgörande för om en gärning bör bedömas som dataintrång av normalgraden eller som grovt dataintrång är i regel också av betydelse för bedömningen av brottets straffvärde. Om de omständigheter som föranleder att

ett dataintrång bedöms som grovt inte beaktas tillräckligt genom brottsrubriceringen ska straffvärdet anses ligga över straffminimum för grovt dataintrång. Det innebär bl.a. att straffvärdet normalt bör anses ligga över straffminimum om flera av de omständigheter som ska beaktas särskilt vid bedömande av om brottet är grovt samtidigt har förelegat. Vid straffvärdebedömningen ska också försvårande eller förmildrande omständigheter enligt 29 kap. 2 och 3 §§ brottsbalken beaktas i skärpande respektive mildrande riktning. Som exempel på en sådan försvårande omständighet kan särskilt nämnas om brottet utgjort ett led i en brottslighet som utövats i organiserad form eller systematiskt eller om brottet föregåtts av särskild planering (29 kap. 2 § 6 brottsbalken). När det gäller it-relaterad brottslighet behöver den inte vara organiserad på samma sätt som ”traditionell” brottslighet för att den ska anses ha utövats i organiserad form eller systematiskt. Olika former av s.k. hackernätverk kan därför i vissa situationer då det är fråga om samfällda eller annars gemensamma attacker falla in under 29 kap. 2 § 6 brottsbalken, även om det inte finns någon på förhand bestämd eller strukturerad samverkan.

När det gäller förhållandet mellan dataintrång och övriga brottsbalksbrott får, som inledningsvis nämnts, detta avgöras enligt sedvanliga principer för bedömningen av konkurrens mellan bestämmelser i brottsbalken med gemensamma tillämpningsområden. De fall då dataintrångsbestämmelsen och bestämmelsen om brytande av post- eller telehemlighet skulle kunna vara samtidigt tillämpliga på ett och samma förfarande är i princip enbart när någon berett sig tillgång till ett elektronisk meddelande som är under befordran av ett telebefordringsföretag. Det följer då av principen om *lex specialis* att det är bestämmelsen om brytande av post- eller telehemlighet som ska tillämpas. Det är svårt att se att en sådan gärning på vilken såväl bestämmelsen om brytande av post- eller telehemlighet som dataintrångsbestämmelsen i teorin skulle kunna vara tillämplig i något fall skulle kunna anses så allvarlig och straffvärd att det skulle kunna bli aktuellt att tillämpa bestämmelsen om grovt dataintrång. I den konkurrenssituation som alltså skulle kunna uppkomma – då någon berett sig tillgång till ett elektronisk meddelande som är under befordran av ett telebefordringsföretag – bör det alltså räcka att med tillämpning av principen om *lex specialis* tillämpa straffbestämmelsen brytande av post- eller telehemlighet.

När det gäller förhållandet mellan dataintrångsbestämmelsen och bestämmelsen om intrång i förvar är det över huvud taget svårt

att tänka sig exempel på när dessa bestämmelser samtidigt skulle kunna vara tillämpliga på ett och samma förfarande. Bestämmelsen om intrång i förvar tar nämligen sikte på att bereda sig tillgång till något fysiskt eller materiellt som förvaras förseglat eller under lås eller på annat sätt tillslutet, exempelvis att bereda sig tillgång till ett brev, dokument eller en annan handling genom att bryta upp en låst skrivbordslåda.

När det gäller konkurrensfrågor i övrigt då det nu införs en särskild straffskala för grovt dataintrång får dessa lösas enligt sedvanliga konkurrensregler. Om det är fråga om konkurrens mellan dataintrångsbrottet och ett annat brott med samma skyddsintresse innebär det normalt att domstolen ska döma för det brott som har den strängare straffskalan (Berggren m.fl., *Brottsbalken En kommentar kap. 1–12*, s. 4:50 d). Sådana konkurrenssituationer kan främst tänkas uppkomma i förhållandena till bestämmelserna om skadegörelse och sabotage. Om det skulle uppkomma andra konkurrenssituationer får domstolen enligt de konkurrensprinciper som gäller i allmänhet göra en prövning i varje enskilt fall.

10 § För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott döms till ansvar enligt vad som sägs i 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt, till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa, *eller till grovt dataintrång*.

Tillägget i paragrafen, som behandlas i avsnitt 9.4, är en konsekvens av att en särskild straffskala för grovt dataintrång införs i 9 c § andra stycket. Tillägget innebär att även försök eller förberedelse till grovt dataintrång är straffbart.

12.3 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

1 kap.

2 § 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,

6. föreläggande enligt 27 kap. 16 § rättegångsbalken,

7. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,

8. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,

9. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,

10. hemlig kameraövervakning,

11. hemlig rumsavlyssning,

12. överförande av frihetsberövade för förhör m.m., och

13. 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.

I paragrafen finns en uttömmande uppräkning av vilka åtgärder som avses med rättslig hjälp enligt lagen. De allmänna överväganden finns i avsnitt 8.4.2.

I *första stycket 6* har tagits in en ny bestämmelse som innebär att rättslig hjälp kan ges med bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken. Det är alltså möjligt att efter ansökan från en annan stat förelägga någon som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften under viss tid (jfr kommentaren till 27 kap. 16 § rättegångsbalken). Till följd av att den nya formen av rättslig hjälp har införts i första stycket 6 har de följande sju punkterna i första stycket fått nya nummer.

2 kap.

1 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–*7*, *10*, *11* och *13* ska 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 *8*, *9* och *12* lämnas enligt de särskilda bestämmelserna i denna lag.

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

I paragrafens första stycke finns en generell regel som innebär att svenska åklagare och domstolar kan bistå den andra staten med de åtgärder som räknas upp i 1 kap. 2 § under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång. Ändringarna i *första stycket* är föranledda av att rättslig hjälp även ska kunna ges med bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken. Denna åtgärd anges i 1 kap. 2 § första stycket 6, varvid de efterföljande uppräknade åtgärderna fått nya punktnummer.

Ändringarna i *andra stycket* är redaktionella och föranledda av att vissa av de uppräknade åtgärderna i 1 kap. 2 § första stycket fått nya punktnummer.

De allmänna övervägandena finns i avsnitt 8.4.2.

2 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *6*, *8* och *12* 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*, *9*–*11* och *13* 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.

Av paragrafen framgår att rättslig hjälp i vissa fall kan lämnas utan att något krav på dubbel straffbarhet – dvs. att gärningen också är straffbar i Sverige – ställs upp. Rättslig hjälp med bevarandeförläggande enligt 27 kap. 16 § rättegångsbalken är, genom hänvisningen till 1 kap. 2 § första stycket 6, en sådan åtgärd som får vidtas utan krav på dubbel straffbarhet. De allmänna övervägandena finns i avsnitt 8.4.2. I övrigt är ändringarna i bestämmelsen enbart redaktionella och beror på att vissa av de åtgärder som räknas upp i 1 kap. 2 § första stycket har fått nya punktnummer.

4 § 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 ska höras,

– namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14, 24 a, *24 c*, 25, 25 b, 25 c, 26 a och 29 §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

Om ärendet är brådskande eller om verkställighet önskas inom viss tidsfrist, ska detta anges och motiveras.

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

Av bestämmelsen framgår vad en ansökan om rättslig hjälp bör innehålla. I *andra stycket* har lagts till en hänvisning till den nya bestämmelsen 4 kap. 24 c § i vilken anges vad en ansökan ytterligare ska innehålla vid ansökan om rättslig hjälp med bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken. Frågan behandlas i avsnitt 8.4.2.

4 kap.

24 c § *En ansökan om föreläggande enligt 27 kap. 16 § rättegångsbalken handläggs av åklagare.*

Av ansökan ska framgå sådana uppgifter som behövs för att åtgärden ska kunna genomföras.

Åklagaren ska genast pröva om det finns förutsättningar för åtgärden. Om åtgärden beslutas ska denna gälla för en period om minst 60 dagar.

Paragrafen är ny. Den innehåller vissa bestämmelser om handläggningen av en ansökan om rättslig hjälp med bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken. De allmänna överväganden finns i avsnitt 8.4.2.

Av *första stycket* framgår att en ansökan om rättslig hjälp med bevarandeföreläggande handläggs av åklagare.

I *andra stycket* finns föreskrifter om ansökans innehåll, vilka kompletterar de allmänna bestämmelserna i 2 kap. 4 §. Av ansökan

ska framgå sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Det måste exempelvis framgå vilka lagrade uppgifter som ska säkras och var och hos vem säkrande begärs.

Av *tredje stycket* framgår att åklagaren genast ska göra en prövning av om förutsättningarna för att meddela ett föreläggande är uppfyllda. Av 2 kap. 1 § följer att åtgärden ska vidtas under de förutsättningar som anges i rättegångsbalken. För det fall föreläggande beslutas ska tiden för bevarande vara minst 60 dagar, så att den ansökande staten får tid på sig att förbereda en ansökan om åtkomst till uppgifterna. Samtidigt gäller den generella regeln i 27 kap. 16 § andra stycket rättegångsbalken att förordnandet inte får gälla längre än 90 dagar, med möjlighet till 30 dagars förlängning om det finns särskilda skäl.

12.4 Förslaget till lag om ändring i lagen (2003:389) om elektronisk kommunikation

6 kap.

5 § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a eller 16 c § *eller om uppgifterna begärts bevarade enligt 27 kap. 16 § rättegångsbalken*.

I paragrafen finns huvudregeln om behandling av trafikuppgifter. Den innebär att när en sådan uppgift inte längre behövs för att överföra ett elektroniskt meddelande måste uppgiften utplånas eller avidentifieras. Paragrafen innehåller dock vissa undantag från huvudregeln.

Paragrafen har kompletterats med ytterligare ett undantag. Om uppgifterna har begärts bevarade enligt 27 kap. 16 § rättegångsbalken gäller inte huvudregeln.

De allmänna övervägandena finns i avsnitt 8.3.2.

16 c § Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 *eller 9*, 27 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

I paragrafen regleras för vilka ändamål uppgifter som har lagrats enligt 16 a § får användas. De allmänna övervägandena finns i avsnitt 8.3.3.

Enligt tillägget ska uppgifter som har lagrats enligt 16 a § även få behandlas för att lämnas ut enligt 22 § första stycket 9. Den enda uppgift som emellertid får lämnas ut enligt den bestämmelsen är uppgift om vilka övriga leverantörer som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken (se kommentaren till 22 §).

16 d § Uppgifter som avses i 16 a § ska lagras i sex månader räknat från den dag kommunikationen avslutades. Vid utgången av denna tid ska den lagringsskyldige genast utplåna dem, om annat inte följer av andra stycket.

Om uppgifter som avses i första stycket begärts utlämnade *eller om uppgifter begärts bevarade enligt 27 kap. 16 § rättegångsbalken* före utgången av den föreskrivna lagringstiden men uppgifterna inte har hunnit lämnas ut *eller tiden för bevarande inte har löpt ut*, ska den lagringsskyldige lagra uppgifterna till dess så har skett och därefter genast utplåna de lagrade uppgifterna.

I paragrafen regleras lagringstidens längd och de åtgärder som ska vidtas från leverantörens sida vid lagringstidens slut. De allmänna övervägandena finns i avsnitt 8.3.2.

I *andra stycket* har lagts till att uppgifter som ska bevaras enligt 27 kap. 16 § rättegångsbalken inte ska utplånas innan tiden för bevarande har löpt ut.

16 g § *Om någon som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § förelagts att bevara viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken gäller vad som sägs i 3 a § om åtgärder för att skydda uppgifter som ska lagras enligt 16 a § även för uppgift som ska bevaras enligt 27 kap. 16 § rättegångsbalken. Vidare gäller vad som sägs i 16 e § om rätt till ersättning för kostnader och i 16 f § om anpassning för utlämnande av uppgifter på motsvarande sätt även för uppgift som ska bevaras enligt 27 kap. 16 § rättegångsbalken.*

Paragrafen, som är ny, har behandlats i avsnitt 8.3.2.

Bestämmelsen innebär att den särskilda bestämmelsen i 3 a § om kvalitet och säkerhet när det gäller de trafikuppgifter som lagrats för brottsbekämpande syften är tillämplig även i de fall då någon

som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § förelagts att bevara viss lagrad uppgift enligt den föreslagna bestämmelsen i 27 kap. 16 § rättegångsbalken. Regeringen eller den myndighet som regeringen bestämmer kan då även, med stöd av 3 a §, ange ytterligare föreskrifter om säkerheten för de uppgifter som ska bevaras.

Bestämmelsen innebär vidare att bestämmelserna om rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut (16 e §) och om anpassning för utlämnande av uppgifter (16 f §) gäller även för uppgifter som omfattas av ett bevarandeföreläggande enligt den föreslagna bestämmelsen i 27 kap. 16 § rättegångsbalken hos någon som är anmälningspliktig enligt 2 kap. 1 § LEK. Ersättning ska betalas till den som bevarat uppgifterna av den myndighet som har begärt uppgifterna. Regeringen eller den myndighet som regeringen bestämmer ska meddela föreskrifter om ersättning.

21 § Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,

2. angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,

5. begäran om utlämnande av uppgift om abonnemang enligt 22 § första stycket 2,

6. föreläggande att bevara uppgifter enligt 27 kap. 16 § rättegångsbalken, och

7. begäran om utlämnande av uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster enligt 22 § första stycket 9.

Paragrafen innehåller regler om tystnadsplikt för leverantörer. De allmänna övervägandena finns i avsnitt 8.3.2 och 8.3.3.

Enligt *punkterna 6 och 7*, som är nya, ska även uppgifter som hänför sig till ett föreläggande att bevara uppgifter enligt den föreslagna bestämmelsen i 27 kap. 16 § rättegångsbalken och till en begäran från myndigheterna att få tillgång till uppgifter om vilka leverantörer som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande omfattas av regleringen.

22 § Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska 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 (2010:1932), 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 ska ingripa mot brottet,

3. uppgift som avses i 20 § första stycket 1 och 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa,

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och 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 som avser 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 ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

7. 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 ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

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, *och*

9. uppgift om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande enligt 27 kap. 16 § första stycket rättegångsbalken till den myndighet som meddelat föreläggandet.

Ersättning för att lämna ut andra uppgifter enligt första stycket 8 än lokaliseringsuppgifter ska vara skälig med hänsyn till kostnaderna för utlämnandet.

Paragrafen innehåller bestämmelser om leverantörers skyldighet att på begäran lämna ut vissa uppgifter utan hinder av tystnadsplikt. De allmänna övervägandena finns i avsnitt 8.3.3.

I *första stycket 9* har tagits in en bestämmelse om att leverantörer ska vara skyldiga att till den myndighet som beslutat om ett bevarandeföreläggande lämna ut uppgift om vilka övriga leverantörer som har deltagit vid överföringen av det meddelande som omfattas av föreläggandet.

Syftet med den nya uppgiftsskyldigheten är att de brottsutredande myndigheterna ska få möjlighet att identifiera vilka leverantörer som deltagit vid överföringen, så att ett föreläggande om bevarande av elektroniska uppgifter enligt 27 kap. 16 § rättegångsbalken kan riktas även mot dessa. Enbart uppgift om vilka leverantörer som har deltagit vid överföringen ska lämnas ut. Ingen annan information, ur vilken exempelvis skulle kunna härledas vem som kommunicerade med vem, får lämnas ut med stöd av den nya bestämmelsen. Den myndighet som har beslutat om bevarandeföreläggandet har endast möjlighet att få reda på från vilken leverantör som meddelandet sändes och – för det fall det har vidaresänts – till vilken leverantör det vidaresändes.

Det ankommer på leverantören att ur den information som denne har tillgång till ta reda på vilka övriga leverantörer är. Har leverantören inte tillgång till informationen kan denna inte heller lämnas ut. Den nya uppgiftsskyldigheten innebär alltså inte något nytt krav på att spara uppgifter.

I första hand kommer uppgifterna att lämnas till åklagar- eller polismyndighet, men om bevarandeföreläggandet meddelats av Tullverket kan uppgifter lämnas ut även till denna myndighet.

Uppgifter om vilka övriga leverantörer är som deltagit vid överföringen av ett meddelande kommer i den övervägande delen av fallen kunna fås fram genom de trafikuppgifter som lagras enligt 16 a §. Leverantörerna har då enligt 16 e § rätt till ersättning för kostnader som uppstår i samband med att uppgift om vilka övriga leverantörer är lämnas ut.

För leverantörernas tystnadsplikt i fråga om utlämnande av uppgifter, se kommentaren till 21 §.

Kommittédirektiv 2011:98

Tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll

Beslut vid regeringssammanträde den 27 oktober 2011

Sammanfattning

Den ökade användningen av datorer och internet har inneburit att det har utvecklats nya brottstyper och nya tillvägagångssätt för att begå brott. De snabba kommunikationsvägarna och möjligheten för den som begår brott att dölja sin identitet på internet innebär stora utmaningar för de brottsbekämpande myndigheterna. Genom användning av internet kan brott begås i flera stater samtidigt och snabbt få stor omfattning och spridning. För att effektivt kunna bekämpa it-relaterade brott krävs därför ett väl fungerande internationellt samarbete. Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll fyller i detta sammanhang en viktig funktion.

En särskild utredare ska analysera behovet av författningsändringar för att Sverige ska kunna tillträda konventionen och tilläggsprotokollet och lämna förslag till de författningsändringar som behövs för att möjliggöra ett svenskt tillträde till instrumenten.

Uppdraget ska redovisas senast den 2 maj 2013.

Bakgrund

Europarådets konvention om it-relaterad brottslighet

Internet har skapat nya möjligheter att snabbt, enkelt och billigt ta del av, hämta in och distribuera stora mängder information. Samtidigt innebär en ökad användning av internet en förhöjd risk för att datorer och deras nätverk används som verktyg för att begå brott. Detta har skapat behov av en samordnad, effektiv kamp över gränserna mot it-relaterad brottslighet. Europarådets konvention om it-relaterad brottslighet (ETS nr 185, konventionen) har utarbetats för att tillgodose det behovet.

Konventionen har följande tre huvudsyften:

1. Åstadkomma en tillnärmning av ländernas nationella straffrätt beträffande vissa gärningar.

2. Säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser behoven av att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta till vara bevisning i elektronisk form.

3. Lägga grunden för ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott.

Konventionen är indelad i fyra kapitel. Dessa innehåller definitioner, bestämmelser om åtgärder som ska vidtas på nationell nivå, bestämmelser om internationellt samarbete och slutbestämmelser.

Sverige undertecknade konventionen den 23 november 2001. Den trädde i kraft den 1 juli 2004. Hittills har 47 stater undertecknat konventionen och 31 stater ratificerat den. Majoriteten av EU:s medlemsstater har ratificerat konventionen liksom de övriga nordiska länderna. Även stater som inte är medlemmar i Europarådet kan ansluta sig till konventionen. Konventionen har ratificerats av USA och undertecknats av Kanada, Japan och Sydafrika.

Frågor om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som begåtts med hjälp av ett datorsystem behandlas i ett tilläggsprotokoll till konventionen av den 28 januari 2003 (tilläggsprotokoll till konventionen om it-relaterad brottslighet om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem, ETS nr 189). Sverige undertecknade protokollet samma dag. Protokollet har två syften. Det ena är att åstadkomma en tillnärmning av den materiella straffrätten i fråga om ovannämnda brott. Det andra är att förbättra det

internationella samarbetet vid bekämpning av sådana brott. Tilläggsprotokollet trädde i kraft den 1 mars 2006.

Europarådets ministerkommitté har antagit förklarande rapporter till såväl konventionen som tilläggsprotokollet.

Bekämpningen av it-relaterad brottslighet är ett prioriterat område för EU. I Stockholmsprogrammet, som anger inriktningen på EU:s arbete inom det rättsliga och inrikes området för femårsperioden 2010–2014, framhålls att medlemsstaterna så snart som möjligt bör ratificera konventionen och att den bör bli den rättsliga referensramen för it-brottslighet på global nivå.

Även inom FN pågår diskussioner om behovet av åtgärder för att förbättra det internationella arbetet mot it-relaterad brottslighet.[1] FN:s kriminalpolitiska kommission (CCPCJ) har tillsatt en expertarbetsgrupp för detta ändamål. En fråga som har diskuterats i arbetsgruppen är om det finns behov av en FN-konvention om it-relaterad brottslighet.

Behovet av en utredning

Frågan om Sverige bör tillträda konventionen och tilläggsprotokollet samt vilka lagändringar som krävs för ett tillträde behandlas i promemorian Brott och brottsutredning i it-miljö (Ds 2005:6). I promemorian görs bedömningen att Sverige bör tillträda såväl konventionen som tilläggsprotokollet. Enligt promemorian uppfyller inte svensk rätt konventionens krav. Det gäller främst på straffprocessrättens område. Promemorian har remissbehandlats. Samtliga remissinstanser som har yttrat sig i frågan har varit positiva till att konventionen och protokollet tillträds. Många remissinstanser har dock pekat på behovet av samordning med andra pågående lagstiftningsärenden och anfört att förslaget brister i överskådlighet. Det har också framförts att förslag som närmare ansluter till konventionens systematik bör övervägas.

Sedan promemorian skrevs har förutsättningarna för bedömningen av om svensk rätt uppfyller konventionens krav väsentligen förändrats. Bland annat har regeringen föreslagit ett genomförande av Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med till-

[1] Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, slutsatser från FN:s kriminalpolitiska kongress i Brasilien i april 2010.

handahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (prop. 2010/11:46). Förslaget innebär att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät åläggs en skyldighet att lagra trafik- och lokaliseringsuppgifter samt uppgifter som behövs för att identifiera en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott. Förslagen i propositionen har vilandeförklarats av riksdagen (bet. 2010/11:JuU14, rskr. 2010/11:189). Regeringen har vidare i en lagrådsremiss den 16 december 2010 föreslagit förändringar i de bestämmelser som rör de brottsbekämpande myndigheternas tillgång till övervaknings- och abonnemangsuppgifter om elektronisk kommunikation. Även när det gäller den materiella straffrätten och de bestämmelser som reglerar det internationella samarbetet har förändringar skett sedan promemorian skrevs.

Det finns mot denna bakgrund behov av att på nytt se över vilka författningsändringar som behövs för att Sverige ska kunna leva upp till kraven i konventionen och tilläggsprotokollet.

Uppdragets allmänna utgångspunkter

Sverige har länge intagit en ledande position i fråga om it-användning. Regeringens ambition är att Sverige ska vara ledande i användningen av it för att nå tillväxt-, välfärds-, demokrati- och klimatmål. Detta förutsätter, vid sidan av bl.a. väl utvecklade säkerhetslösningar, en straffrättslig lagstiftning som ger ett gott skydd mot missbruk av den nya tekniken och en processrättslig lagstiftning som ger goda möjligheter att effektivt utreda och lagföra it-relaterade brott.

Teknikutvecklingen har skapat nya möjligheter att begå brott utan att gärningsmannen befinner sig i det land där brottet får effekt. Det finns också stora möjligheter för den som begår ett brott att dölja sin identitet. It-relaterade brott kan snabbt få stor omfattning och spridning. Bevis kan utplånas och ekonomiskt utbyte av brott flyttas mellan länder på mycket kort tid. Vissa brott, t.ex. internetrelaterade barnpornografibrott, kan bara utredas genom att de brottsbekämpande myndigheterna får tillgång till uppgifter om elektronisk kommunikation. Detta medför nya utmaningar för de brottsbekämpande myndigheterna och ett ökat behov av ett effektivt internationellt samarbete. Sverige bör delta aktivt i detta samarbete.

Konventionen och tilläggsprotokollet utgör en internationell överenskommelse i fråga om det grundläggande behovet av åtgärder för att motverka it-relaterad brottslighet. Utgångspunkten är att Sverige bör ratificera konventionen och tilläggsprotokollet. För att det ska vara möjligt krävs vissa lagändringar.

De anslutande staterna avgör själva på vilket sätt konventionen ska genomföras i nationell rätt. Regleringen av myndigheternas tillgång till uppgifter ska enligt konventionen utformas så att de ger ett tillfredsställande skydd för mänskliga fri- och rättigheter enligt bl.a. Europakonventionen.

Vad ska utredas?

Uppdragets omfattning

Utredaren ska i fråga om konventionen och tilläggsprotokollet

- göra en genomgång av bestämmelserna och analysera i vilka avseenden det finns behov av författningsändringar eller andra förändringar för att Sverige ska leva upp till kraven i konventionen och tilläggsprotokollet,
- ta ställning till i vilken utsträckning Sverige bör utnyttja möjligheten att göra förbehåll, t.ex. genom att ange att vissa gärningar inte ska vara straffbelagda eller att vissa utredningsåtgärder bara ska kunna tillämpas för vissa brott eller brottstyper (artikel 42 i konventionen respektive artikel 12 i tilläggsprotokollet), att avge förklaring att ytterligare rekvisit uppställs (artikel 40) eller att specificera för vilket eller vilka territorier som konventionen ska gälla (artikel 37), samt
- lämna förslag till de författningsändringar eller andra förändringar som krävs för att Sverige ska kunna tillträda konventionen och tilläggsprotokollet.

Utredaren får också lämna sådana närliggande förslag till författningsändringar som bedöms nödvändiga för att uppdraget ska kunna genomföras på ett fullgott sätt. I uppdraget ingår inte att överväga ändringar i grundlagarna.

De närmare förutsättningarna för uppdraget i fråga om anpassningen av den straff- respektive processrättsliga regleringen och den

reglering som rör internationellt rättsligt samarbete utvecklas i kommande avsnitt.

Särskilt om anpassningen av den straffrättsliga regleringen

Syftet med de straffrättsliga bestämmelserna i konventionen är att förbättra möjligheterna att förhindra och förebygga it-relaterade brott genom att skapa en gemensam minimistandard för sådana brott. Genom att tillnärma straffrätten minskar risken att brottsligheten flyttas från en stat till en annan med mindre sträng lagstiftning. Vidare underlättas det internationella samarbetet i fråga om utlämning och rättslig hjälp.

I artiklarna 2–6 behandlas inledningsvis sådana gärningar som är riktade mot datorsystem och datorbehandlingsbara uppgifter. I artiklarna 7 och 8 behandlas s.k. datorrelaterade brott. Datorrelaterad förfalskning regleras i artikel 7 och datorrelaterat bedrägeri behandlas i artikel 8. Artikel 9 rör barnpornografibrott och artikel 10 brott mot upphovsrätt och till upphovsrätten närstående rättigheter. Artiklarna 11–13 behandlar försök och medhjälp till brott, juridiska personers ansvar samt påföljder. Av artiklarna framgår i vilken utsträckning en stat får förbehålla sig rätten att inte straffbelägga vissa gärningar eller uppställa vissa begränsande krav i fråga om vilka gärningar som är straffbara. Dessutom får ringa brott undantas från kriminalisering, även om detta inte har kommit till direkt uttryck i konventionstexten (p. 37 i den förklarande rapporten till konventionen).

Inom EU antogs i februari 2005 ett rambeslut om angrepp mot informationssystem. Rambeslutet syftar till att tillnärma medlemsstaternas straffrättsliga lagstiftning när det gäller angrepp mot informationssystem och därigenom förbättra samarbetet mellan rättsliga och andra myndigheter och bidra till kampen mot organiserad brottslighet och terrorism. Konventionen om it-relaterad brottslighet har till stor del utgjort förebild för rambeslutet. Rambeslutet innehåller bestämmelser om vilka handlingar som ska vara straffbelagda som angrepp mot informationssystem. Dessutom finns bestämmelser om bl.a. påföljder för brotten, ansvar och påföljder för juridiska personer, domsrätt och utbyte av uppgifter medlemsstaterna emellan. Vid genomförandet av rambeslutet i svensk rätt infördes ett utvidgat straffansvar i bestämmelsen om dataintrång i brottsbalken (prop.

2006/07:66). Inom EU pågår förhandlingar om ett direktiv som ska ersätta rambeslutet.

It-förfalskningsutredningen har i betänkandet Urkunden i tiden – en straffrättslig anpassning (SOU 2007:92) lämnat förslag som kan innebära att kravet på kriminalisering i artikel 7 i konventionen (datorrelaterad förfalskning) uppfylls. Förslagen bereds för närvarande i Regeringskansliet.

Tilläggsprotokollet behandlar frågan om kriminalisering av gärningar av rasistisk eller främlingsfientlig natur som begås med hjälp av datorsystem. Tilläggsprotokollet aktualiserar därmed frågor om informations-, yttrande- och tryckfrihet. Både tryckfrihetsförordningen och yttrandefrihetsgrundlagen straffbelägger gärningar av rasistisk och främlingsfientlig natur. Motsvarande allmänna brott finns i brottsbalken. Tryckfrihetsförordningen och yttrandefrihetsgrundlagen innehåller också processuella bestämmelser som delvis avviker från rättegångsbalkens regler.

Protokollet överensstämmer i många delar med EU:s rambeslut 2008/913/RIF om bekämpande av vissa former av och uttryck för rasism och främlingsfientlighet enligt strafflagstiftningen. Regeringen har gjort bedömningen att svensk rätt uppfyller rambeslutets krav (Ju2008/3200/L5).

Särskilt om anpassningen av den processrättsliga regleringen

De processrättsliga reglerna i konventionen är indelade i avsnitt med utgångspunkt i typen av åtgärd. Avdelningen inleds med allmänna bestämmelser som är gemensamma för hela det processrättsliga avsnittet (artiklarna 14 och 15). Härefter följer ett avsnitt om skyndsamt säkrande av lagrade uppgifter (artiklarna 16 och 17), skyldighet att lämna uppgifter (artikel 18), husrannsakan och beslag (artikel 19) samt insamling i realtid av uppgifter (artiklarna 20 och 21).

Konventionen innehåller bestämmelser om att behöriga myndigheter ska kunna ålägga t.ex. teleoperatörer att bevara särskilt angivna datorbehandlingsbara uppgifter orubbade. Den som ska bevara uppgifterna ska kunna åläggas en skyldighet att hemlighålla att åtgärden har ägt rum. Trafikuppgifter ska sedan skyndsamt kunna röjas för behöriga myndigheter (artiklarna 16 och 17). Med trafikuppgifter avses i konventionen varje typ av datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av datorsystem och som genereras av ett datorsystem som ingår i kommu-

nikationskedjan och som anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst. Det är alltså uppgifter som svarar på frågor som vem som kommunicerade med vem vid en viss tidpunkt, var det skedde, på vilket sätt (t.ex. genom e-post) och hur länge.

Den som innehar särskilt angivna datorbehandlingsbara uppgifter ska kunna åläggas att lämna ut dessa (artikel 18). De brottsbekämpande myndigheterna ska också enligt konventionen kunna ålägga en person med kunskap om ett datorsystem att lämna uppgifter om lösenord m.m. (artikel 19.4).

Utgångspunkten är att de åtgärder som anges i konventionen ska kunna tillämpas på

- de brott som omfattas av konventionens artiklar 2–11,
- övriga brott som begåtts med hjälp av datorteknik och
- bevisning i elektronisk form (artikel 14).

I konventionen görs en uppdelning mellan möjligheten att inhämta uppgifter om elektronisk kommunikation i realtid och att inhämta uppgifter som avser förfluten tid. För inhämtning i realtid (artiklarna 20 och 21) gäller att parterna får förbehålla sig rätten att endast tillämpa sådana åtgärder på brott eller brottstyper som anges i förbehållet (artikel 14.3). Motsvarande möjlighet till förbehåll saknas i fråga om inhämtning av uppgifter avseende förfluten tid.

I svensk rätt görs normalt ingen skillnad mellan olika typer av bevisning. Det innebär att det inte finns generella legala begränsningar förknippade med bevisning i elektronisk form. Till skillnad från konventionens bestämmelser görs i de svenska bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning ingen åtskillnad vad gäller möjligheten att inhämta uppgifter i realtid respektive uppgifter som avser förfluten tid (jfr dock förslagen i lagrådsremissen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation). Hemlig teleavlyssning förutsätter normalt att det för brottet inte är föreskrivet lindrigare straff än fängelse i två år (27 kap. 18 § andra stycket rättegångsbalken). Uppgifter om telemeddelanden är i en brottsutredning åtkomliga med stöd av reglerna om hemlig teleövervakning. Även användningen av hemlig teleövervakning är begränsad till vissa brott. Hemlig teleövervakning får användas vid misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader, vissa särskilt angivna

brott (bl.a. dataintrång och barnpornografibrott) och försök, förberedelse eller stämpling till dessa brott om sådan gärning är belagd med straff (27 kap. 19 § andra stycket rättegångsbalken). Hos en teleoperatör får inte andra straffprocessuella tvångsmedel (t.ex. husrannsakan och beslag) eller edition användas för att få fram uppgifter vars åtkomst regleras i bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning.

Sådana uppgifter om telemeddelanden som finns lagrade hos operatörer och som avser annat än innehållet kan enligt gällande rätt i viss utsträckning även lämnas ut med stöd av lagen (2003:389) om elektronisk kommunikation (6 kap. 22 § första stycket 3), under förutsättning att det för brottet inte är föreskrivet lindrigare straff än fängelse två år. Denna möjlighet har dock i lagrådsremissen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation föreslagits ersättas med annan reglering. Lagrådsremissen bereds för närvarande inom regeringskansliet.

Enligt konventionen ska det också vara tillåtet att framställa och behålla en kopia av datorbehandlingsbara uppgifter som har säkrats (artikel 19.3 b). Förundersökningsutredningen (Ju 2009:07) har nyligen gjort en översyn av hur reglerna om beslag tillämpas i it-miljö och föreslagit en lagreglering i fråga om kopiering av beslagtaget material (SOU 2011:45).

Bestämmelserna i konventionen har utarbetats för att motsvara en miniminivå i fråga om behovet av utredningsåtgärder i respektive stat för att effektivt kunna bekämpa it-relaterad brottslighet. Vissa av åtgärderna i konventionen motiveras vidare av att de ska erbjuda ett mindre ingripande alternativ till husrannsakan och beslag (förklarande rapporten p. 170). Staterna ska själva ta ställning till på vilket sätt konventionens bestämmelser ska genomföras i nationell rätt och de närmare förutsättningarna för tillämpningen av åtgärderna. Staterna ska enligt konventionen se till att de nationella bestämmelserna ger ett tillfredsställande skydd för mänskliga rättigheter enligt bl.a. Europakonventionen (artikel 15).

Bedömningen av i vilken mån de utredningsåtgärder som omfattas av konventionen kan vidtas enligt svensk rätt och om de kan tillämpas på de förfaranden och under de förutsättningar som anges i konventionen kan påverkas av de förslag som lämnats i lagrådsremissen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Utredaren ska, i den mån analysen föranleder förslag om nya straffprocessuella tvångsmedel eller ändringar i befintliga tvångs-

medel, utforma förslagen på ett sådant sätt att befogenheten att använda aktuellt tvångsmedel är proportionerlig i förhållande till det intrång i enskildas integritet som befogenheten innebär. Det är vidare angeläget att åstadkomma en så klar och överblickbar tvångsmedelsreglering som möjligt. Vid utarbetande av förslag till nya bestämmelser ska utredaren ta hänsyn till den grundläggande systematiken i regleringen och den vidare beredningen av lagrådsremissen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Särskilt om anpassningen av regleringen som rör internationellt rättsligt samarbete

Bestämmelserna om internationellt samarbete utgör en betydande del av konventionen (kapitel tre). De är uppdelade i två avsnitt, ett allmänt avsnitt där de grundläggande principerna läggs fast och ett med särskilda bestämmelser om vissa tvångsåtgärder m.m. Det allmänna avsnittet är uppdelat i olika avdelningar som behandlar allmänna principer för hela det rättsliga samarbetet enligt konventionen (artikel 23), principer som gäller för utlämning (artikel 24) respektive rättslig hjälp (artiklarna 25 och 26) samt bestämmelser beträffande förfarandet vid framställningar om rättslig hjälp (artiklarna 27 och 28). Det andra avsnittet är indelat i avdelningar som behandlar rättslig hjälp med provisoriska åtgärder (artiklarna 29 och 30), rättslig hjälp med utredningsbefogenheter (artiklarna 31 och 34) samt nätverk av kontaktpunkter (artikel 35).

Artiklarna om internationellt samarbete har på motsvarande sätt som bestämmelserna om bevisinhämtning ett vidare tillämpningsområde än enbart de brott som anges i artiklarna 2–11. Samarbetet i enlighet med konventionens bestämmelser omfattar 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.

Med utgångspunkt i konventionen, internationella överenskommelser om rättsligt samarbete och andra överenskommelser samt den nationella lagstiftningen, ska 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.

I svensk rätt är reglerna om internationellt rättsligt samarbete uppdelade i olika författningar bl.a. med utgångspunkt i formen av

samarbete. Regler om utlämning för brott finns t.ex. i lagen (1957:668) om utlämning för brott och, när det gäller förhållandet mellan EU:s medlemsstater, i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder. Överförande av lagföring mellan stater regleras genom lagen (1976:19) om internationellt samarbete rörande lagföring för brott. Det finns också lagar som är tillämpliga på särskilda former av samarbete mellan EU:s medlemsstater, t.ex. lagen (2005:500) om erkännande och verkställighet inom EU av frysningsbeslut. Tyngdpunkten i konventionen när det gäller det internationella samarbetet rör dock olika aspekter av rättslig hjälp. Regler om rättslig hjälp i brottmål finns bl.a. i lagen (2000:562) om internationell rättslig hjälp i brottmål.

När svenska åklagare och domstolar lämnar internationell rättslig hjälp, ska de regler som gäller för ett motsvarande svenskt förfarande tillämpas med den modifiering som följer av specialregleringen för sådan hjälp. Det innebär att ändringar som sker i de ordinarie svenska reglerna också får genomslag för hanteringen av ärenden om rättslig hjälp. I vissa fall leder sådana ändringar också till att den aktuella specialregleringen måste ändras. Det kan även i övrigt finnas behov av ändringar med hänsyn till konventionens krav.

När lagen om internationell rättslig hjälp i brottmål infördes gavs den ett vidare tillämpningsområde än vad som krävdes med hänsyn till då gällande internationella åtaganden. Syftet var att för framtiden skapa utrymme för ett utvidgat internationellt samarbete. Utgångspunkten för regleringen är att alla åtgärder som är möjliga att vidta i en svensk förundersökning också ska vara tillgängliga för en annan stat efter en ansökan om rättslig hjälp, oavsett om bistånd med åtgärden föreskrivs i en internationell överenskommelse eller inte. Eventuella förslag till ändringar i lagen med anledning av tillträdet till konventionen måste vara anpassade till denna grundläggande systematik i regleringen. Utredaren måste också beakta redan ingångna internationella åtaganden som kan beröras av ändringsförslagen.

Uppdragets genomförande

Lagstiftning i andra länder

Utredaren ska, i den utsträckning det bedöms ha betydelse för uppdragets genomförande, informera sig om genomförandet av konventionen i andra med Sverige jämförbara länder.

Ekonomiska konsekvenser

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa i vilken utsträckning resursutnyttjandet i rättsväsendet kan bli effektivare genom förslagen.

Samråd och redovisning

Vid genomförandet av uppdraget ska utredaren samråda med Utredningen om vissa hemliga tvångsmedel (Ju 2010:08), Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden och Post- och telestyrelsen samt med andra myndigheter i den utsträckning utredaren finner lämpligt.

Utredaren ska också följa arbetet inom Regeringskansliet med bl.a. betänkandena Urkunden i tiden (SOU 2007:92) och Förundersökning – objektivitet, beslag, dokumentation m.m. (SOU 2011:45), med Utlämningsutredningens (Ju 2009:16) kommande förslag samt med lagrådsremissen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation. Utredaren ska också följa relevant arbete inom EU, bl.a. förhandlingarna om förslaget till direktiv om angrepp mot informationssystem (KOM[2010] 517), förslaget till direktiv om en europeisk utredningsorder (2010/C 165/02) och utvärderingen av Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG. Utredaren ska slutligen följa arbetet i riksdagen med de vilande lagförslagen i propositionen om genomförandet av sistnämnda direktiv (bet.

2010/11:JuU14, rskr. 2010/11:189) och Yttrandefrihetskommitténs arbete (dir 2007:76).

Uppdraget ska redovisas senast den 2 maj 2013.

(Justitiedepartementet)

Kommittédirektiv 2012:102

Tilläggsdirektiv till Utredningen om tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll (Ju 2011:12)

Beslut vid regeringssammanträde den 11 oktober 2012

Sammanfattning av tilläggsuppdraget

Utredningen om it-brottskonventionen (Ju 2011:12) ska utöver vad som framgår av redan beslutade kommittédirektiv

- analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och upphävande av rambeslut 2005/222/RIF, och
- överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem.

Utredningstiden förlängs. Uppdraget ska i stället slutredovisas senast den 3 juni 2013.

Utredningens nuvarande uppdrag

Regeringen beslutade den 27 oktober 2011 kommittédirektiv om tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll (dir. 2011:98). Utredningen har tagit namnet

Utredningen om it-brottskonventionen (Ju 2011:12). I utredningens uppdrag ingår att analysera behovet av författningsändringar för att Sverige ska kunna tillträda konventionen och dess tilläggsprotokoll och lämna förslag till de författningsändringar som behövs för att möjliggöra ett svenskt tillträde till instrumenten.

Tilläggsuppdraget

EU-direktivet om angrepp mot informationssystem

Inom EU pågår förhandlingar om ett direktiv om angrepp mot informationssystem (Europaparlamentets och rådets direktiv om angrepp mot informationssystem och upphävande av rambeslut 2005/222/RIF). Direktivet syftar till att ytterligare närma medlemsstaternas strafflagstiftning till varandra på området för angrepp mot informationssystem. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna. Tyngdpunkten i direktivet utgörs av materiella straffrättsliga bestämmelser. Efter artikel 1 och 2 som innehåller en beskrivning av syftet med direktivet och definitioner av vissa begrepp, behandlas i artiklarna 3–7 vilka gärningar som ska utgöra brott, om de utförs uppsåtligen och orättmätigt. Dessa gärningar är olagligt intrång i informationssystem (artikel 3), olaglig systemstörning (artikel 4), olaglig datastörning (artikel 5), olaglig avlyssning (artikel 6) och vissa åtgärder med verktyg som används för att begå brott (artikel 7). I artikel 8 anges att anstiftan av och medhjälp till sådana gärningar som utgör brott enligt direktivet ska straffbeläggas. Det anges även vilka gärningar som ska straffbeläggas på försöksnivå. Artikel 9 innehåller både generella och artikelspecifika bestämmelser om vilka påföljder som ska kunna dömas ut för brotten i direktivet. Artikel 10 har under förhandlingarna utgått ur utkastet till direktiv. I artiklarna 11 och 12 regleras juridiska personers ansvar samt påföljder för juridiska personer. Jurisdiktionsfrågor regleras i artikel 13. Därefter följer i artikel 14 bestämmelser om informationsutbyte och i artikel 15 bestämmelser om övervakning och statistik. Direktivet avslutas med bestämmelser om ersättande av 2005 års rambeslut, införlivande och om rapporteringsskyldighet m.m. (artiklarna 16–20).

Förhandlingarna om direktivet är i allt väsentligt slutförda. Det återstår för EU:s institutioner att formellt anta den text som har

godkänts av företrädare för rådet och Europaparlamentet (dok. 11399/12). Efter att direktivet antas har medlemsstaterna två år på sig att genomföra det.

Direktivets bestämmelser, i synnerhet på straffrättens område, överensstämmer till stor del med dem som finns i Europarådets konvention om it-relaterad brottslighet. De lagändringar som kan föranledas av direktivet är därför sådana att de sannolikt behövs även för att tillträda konventionen. Mot denna bakgrund och med beaktande av den tid som Sverige har på sig att genomföra direktivet efter att det antas, finns det skäl att ge Utredningen om it-brottskonventionen i uppdrag att även

- analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra det kommande men ännu inte formellt antagna direktivet om angrepp mot informationssystem.

Straffskalorna för angrepp mot informationssystem

Artikel 9 i direktivet innehåller, till skillnad från konventionen, specifika bestämmelser om straffskalornas utformning när det gäller olika former av angrepp mot informationssystem. Förutom att brotten i direktivet generellt ska ha påföljder som är effektiva, proportionerliga och avskräckande fordras att samtliga brott, undantaget osjälvständiga brottsformer, ska ha en straffskala med ett lägsta maximistraff på två år.

För brotten olaglig systemstörning (artikel 4) och olaglig datastörning (artikel 5) krävs dessutom ett lägsta maximistraff på tre år när ett stort antal informationssystem har påverkats genom användning av ett verktyg som har utformats primärt för detta syfte. För dessa brott ställs slutligen ett krav på ett lägsta maximistraff på fängelse i fem år under tre förutsättningar:

- (a) att brottet har begåtts inom ramen för en kriminell organisation,
- (b) att brottet har orsakat allvarlig skada, eller
- (c) att brottet har begåtts mot ett kritiskt informationsinfrastruktursystem.

I brottsbalken finns primärt två brott som bedöms som centrala när det gäller att uppfylla flera av de olika former av angrepp mot informationssystem som beskrivs i direktivet: brytande av post- eller telehemlighet (4 kap. 8 § brottsbalken) och dataintrång (4 kap. 9 c § brottsbalken). Dessa brott har straffskalor som sträcker sig från böter till fängelse i högst två år. Det finns redan mot den bakgrunden ett behov av att göra överväganden om straffskalornas utformning för dessa brott.

Straffskalan för brytande av post- eller telehemlighet har varit oförändrad sedan brottsbalkens tillkomst. Även dataintrångsbestämmelsen har samma straffskala som när bestämmelsen först infördes i datalagen (1973:289), även om den ändrats i sak vid ett flertal tillfällen.

Sedan brottsbalkens och datalagens tillkomst har det skett en betydande samhällsutveckling och informationssystem har i dag en ojämförligt större betydelse i samhället än när bestämmelserna infördes. Det finns tecken på att utvecklingen går mot allt farligare och mer storskaliga angrepp mot informationssystem, till exempel intrång i eller överbelastningsattacker mot bankers och myndigheters informationssystem. Angreppen begås med sofistikerade metoder och kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och kommunikation. De kan också leda till förlust eller förvanskning av hemlig eller i övrigt integritetskänslig information. Många gånger kan ett sådant beteende träffas av straffansvaret för sabotage i 13 kap. 4 § brottsbalken. Beroende på omständigheterna, t.ex. att skadan i och för sig är omfattande men av tillfällig karaktär eller att den infrastruktur som skadas inte utgör för samhället viktig egendom, kan emellertid vissa mycket straffvärda beteenden falla utanför sabotagebestämmelsens tillämpningsområde. Regeringen anser därför att det finns anledning att – även vid sidan av vad som bedöms nödvändigt för att genomföra direktivet – överväga att skärpa straffskalorna för brytande av post- eller telehemlighet och dataintrång.

Utredaren ska mot den bakgrunden

- överväga behovet av och – om det finns anledning till det – lämna förslag till skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem, och

- redovisa sin bedömning av om en sådan straffskärpning bör ske enbart genom förändringar av straffskalorna eller om särskilda straffskalor för grova brott bör införas samt beskriva de straffrättsliga och systematiska konsekvenserna av dessa alternativ.

Arbetets bedrivande och redovisning av uppdraget

Förslagens konsekvenser ska redovisas enligt 14–15 a §§ kommittéförordningen.

Utredningstiden förlängs. Uppdraget ska i stället slutredovisas senast den 3 juni 2013.

(Justitiedepartementet)

Europarådets konvention om it-relaterad brottslighet

(Inofficiell översättning)

Europarådets konvention om it-relaterad brottslighet (ETS 185)

Budapest den 23 november 2001

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 ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska innehas för att straffansvar ska gälla.

2. Denna artikel ska 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 ska 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 ska 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 ska 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 ska gälla.

Artikel 8 – Datorrelaterat bedrägeri

Varje part ska 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 ska 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 ska 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 ska termen *minderårig* innefatta alla personer under 18 års ålder. En part får dock kräva en lägre åldersgräns, som inte ska 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 ska 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 ska 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 rättigheter 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 ska 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 ska 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 ska vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att juridiska personer kan ställas till ansvar för gärningar som straffbeläggs i enlighet med denna konvention, 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 ska varje part vidta nödvändiga åtgärder för att tillse att en juridisk person kan ställas till ansvar när bristande övervakning eller kontroll som ska 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 ska inte inverka på straffansvaret för de fysiska personer som har gjort sig skyldiga till brottet.

Artikel 13 – Påföljder och åtgärder

1. Varje part ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska vara införlivad.

2. Sådana villkor och garantier ska, 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, ska 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 ska vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att dess behöriga myndigheter genom förelägganden eller på liknande sätt ska 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, ska 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 ska vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga den som har de datorbehandlingsbara uppgifterna i sin vård eller en sådan annan person som ska 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 ska gälla för de befogenheter och förfaranden som avses i denna artikel.

Artikel 17 – Skyndsamt säkrande och partiellt röjande av trafikuppgifter

1. Varje part ska i fråga om trafikuppgifter som ska 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 ska kunna identifiera tjänsteleverantörerna och den väg på vilken meddelandet överfördes.

2. Bestämmelserna i artiklarna 14 och 15 ska 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 ska 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 besittning 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 ska 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 ska 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 ska 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 ska kunna utvidga husrannsakan eller det liknande sättet till att bereda sig åtkomst till detta andra system.

3. Varje part ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska gälla för de befogenheter och förfaranden som avses i denna artikel.

Artikel 21 – Avlyssning av innehållsuppgifter

1. Varje part ska 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 ska 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 ska gälla för de befogenheter och förfaranden som avses i denna artikel.

Avsnitt 3 – Domsrätt

Artikel 22 – Domsrätt

1. Varje part ska vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att utöva domsrätt över brott som straffbeläggs 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 ska 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, ska de berörda parterna, om det är lämpligt, samråda för att avgöra vilken domsrätt som är den lämpligaste för lagföring.

Kapitel III – Internationellt samarbete

Avsnitt 1 – Allmänna principer

Avdelning 1 – Allmänna principer för internationellt samarbete

Artikel 23 – Allmänna principer för internationellt samarbete

Parterna ska 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 ska 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, ska 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 ska anses tillhöra de utlämningsbara brotten i ett utlämningsavtal som gäller mellan 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 ska föreligga ska erkänna de brott som avses i punkt 1 i denna artikel som utlämningsbara brott mellan dem.

5. För utlämning ska 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, ska 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 ska 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 ska 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 ska upprätta och föra en aktuell förteckning över de myndigheter som utsetts på detta sätt av parterna. Varje part ska 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 ska 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 ska 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 ska godta och besvara framställningar genom sådana snabba kommunikationsmedel.

4. Om inte annat uttryckligen föreskrivs i artiklarna i detta kapitel, ska 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, ska 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 ska hemlighållas eller endast användas på vissa villkor. Om den mottagande parten inte kan tillmötesgå en sådan begäran, ska den meddela den förstnämnda parten, som då ska 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 ska 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 ska 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 ska utse en eller flera centralmyndigheter som ska 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 ska kommunicera direkt med varandra.

c) Varje part ska 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 ska upprätta och föra en aktuell förteckning över de centralmyndigheter som utsetts på detta sätt av parterna. Varje part ska tillse att uppgifterna i förteckningen alltid är riktiga.

3. Framställningar om ömsesidig rättslig hjälp enligt denna artikel ska 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, ska 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 ska ofördröjligen underrätta den begärande parten om utfallet av en framställning om hjälp. Skälen för avslag eller uppskjutande av hjälpen ska anges. Den anmodade parten ska också underrätta den begärande parten om de skäl som omöj-

liggör 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, ska den ofördröjligen meddela den begärande parten, som då ska avgöra om framställningen ändå ska 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 ska 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, ska 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 ska ställas direkt till dess centralmyndighet.

Artikel 28 – Sekretess och begränsningar i fråga om användning

1. Bestämmelserna i denna artikel ska 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 ska 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, ska den genast meddela den andra parten, som då ska 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 över-

lämna 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 ska innehålla följande:

a) Namnet på den myndighet som begär säkrandet.

b) Den gärning som är föremål för brottsutredning eller lagföring och ett sammandrag av omständigheterna.

c) De lagrade datorbehandlingsbara uppgifter som ska 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, ska 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 ska 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 villkoret om dubbel straffbarhet inte kan uppfyllas när uppgifterna ska 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, ska den ofördröjligen meddela den begärande parten, som då får avgöra om framställningen ändå ska verkställas.

7. Ett säkrande som verkställs som svar på en framställning som avses i punkt 1 i denna artikel ska gälla under en period om minst 60 dagar, för att den begärande parten ska kunna överlämna en framställning om husrannsakan eller liknande åtkomst, beslag eller liknande säkringsåtgärd eller röjande av uppgifterna. Sedan en sådan framställning mottagits, ska 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, ska den anmodade parten snabbt röja en tillräcklig mängd trafikuppgifter för den begärande parten för att identifiera tjänsteleverantören 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 ska 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 ska 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 ska 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, ska för denna hjälp gälla de villkor och förfaranden som anges i den nationella lagstiftningen.

2. Varje part ska 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 ska, 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 ska utse en kontaktpunkt som ska 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 ska 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 ska 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, ska kontaktpunkten tillse att den är i stånd att skyndsamt samverka med en eller flera sådana myndigheter.

3. Varje part ska tillse att utbildad och välutrustad personal är tillgänglig för att underlätta nätverkets verksamhet.

Kapitel IV – Slutbestämmelser

Artikel 36 – Undertecknande och ikraftträdande

1. Denna konvention ska stå öppen för undertecknande av Europarådets medlemsstater och de icke-medlemsstater som har deltagit i utarbetandet av konventionen.

2. Denna konvention ska ratificeras, godtas eller godkännas. Ratifikations-, godtagande- eller godkännandeinstrument ska 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 konventionsstaterna 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 ska 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 ska 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, ska 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, ska de göra detta på ett sätt som inte är oförenligt med konventionens syften och principer.

3. Ingenting i konventionen ska 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 ska generellt sörja för vidsträckta och effektiva rättsliga medel för att de åtgärder som avses i kapitel II ska 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, ska 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 general-

sekreteraren mottog meddelandet. Om det i meddelandet anges att återtagandet av ett förbehåll ska börja gälla den dag som anges i meddelandet och denna dag infaller senare än den dag då generalsekreteraren mottog meddelandet, ska återtagandet gälla från den senare dagen.

2. En part som har gjort ett förbehåll som avses i artikel 42 ska 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 ska 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 ska tillställas Europarådets kommitté för brottsfrågor, som ska avge yttrande över den föreslagna ändringen till ministerkommittén.

3. Ministerkommittén ska 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 ska meddelas parterna för godtagande.

5. En ändring som har antagits i enlighet med punkt 3 i denna artikel ska 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 ska hållas underrättad om tolkningen och tillämpningen av konventionen.

2. Om en tvist skulle uppstå mellan parter om tolkningen eller tillämpningen av denna konvention, ska 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 ska vara bindande för parterna, eller till Internationella domstolen, efter överenskommelse mellan de berörda parterna.

Artikel 46 – Samråd mellan parterna

1. Parterna ska 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 ska fortlöpande informeras om utfallet av det samråd som avses i punkt 1 ovan.

3. Europarådets kommitté för brottsfrågor ska 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 ska 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, ska kostnader som uppstår vid genomförandet av bestämmelserna i punkt 1 ovan bäras av parterna på ett sätt som de ska komma överens om.

5. Parterna ska 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 ska 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 ska deponeras i Europarådets arkiv. Europarådets generalsekreterare ska 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.

Tilläggsprotokoll till konventionen om it-relaterad brottslighet om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem

(Inofficiell översättning)

Tilläggsprotokoll till konventionen om it-relaterad brottslighet om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem (ETS 189)

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 Europaråds-

konventionerna 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, här-

stamning, nationellt eller etniskt ursprung liksom även trosbekännelse, under förebärande av något av de förstnämnda karakteristika.

2. De termer och uttryck som används i protokollet ska tolkas på samma sätt som i konventionen.

Kapitel II – Åtgärder som ska vidtas på nationell nivå

Artikel 3 – Spridande av rasistiskt och främlingsfientligt material med hjälp av datorsystem

1. Varje part ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska i tillämpliga delar gälla detta protokoll.

2. Parterna ska 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 ska 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 ska 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 ska 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 ska 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 ska 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 ska börja gälla en dag som anges där, och denna dag infaller efter den dag då generalsekreteraren mottog meddelandet, ska 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 ska 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 ska 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 ska deponeras i Europarådets arkiv. Europarådets generalsekreterare ska 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.

EUROPEISKA UNIONENS RÅD

Bryssel den 21 juni 2012 (4.7)
(OR. en)

SN 2923/12

Interinstitutionellt ärende:
2010/0273 (COD)

Slutlig 2012-08-10, CL

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) nr …/2012

av den

om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF

———————

BILAGA

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 83.1,

med beaktande av Europeiska kommissionens förslag[1],

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[2],

med beaktande av Regionkommitténs yttrande,

i enlighet med det ordinarie lagstiftningsförfarandet[3], och

av följande skäl:

(1) Syftet med detta direktiv är att tillnärma medlemsstaternas straffrättsliga lagstiftning på området angrepp mot informationssystem, genom att fastställa minimiregler om fastställande av brottsrekvisit och påföljder inom detta område, och att förbättra samarbetet mellan behöriga myndigheter, inbegripet polismyndigheter och andra specialiserade brottsbekämpande organ i medlemsstaterna samt unionen behöriga specialiserade organ såsom Eurojust, Europol och dess europeiska it-

[1] EUT C
[2] EUT C
[3] Europaparlamentets ståndpunkt av den … (ännu ej offentliggjord i EUT) och rådets beslut av den...

brottscentrum samt Europeiska byrån för nät- och informationssäkerhet (ENISA).

(1a) Informationssystem är av central betydelse för det politiska, sociala och ekonomiska samspelet i unionen. Samhället är starkt och i allt högre grad beroende av sådana system. Att dessa system fungerar smidigt och säkert i unionen är en förutsättning för utvecklingen av den inre marknaden och för en konkurrenskraftig och innovativ ekonomi. Säkerställande av lämpliga skyddsnivåer för informationssystem bör ingå i ett effektivt övergripande ramverk med förebyggande åtgärder, tillsammans med straffrättsliga åtgärder mot it-brott.

(2) Angrepp mot informationssystem, särskilt angrepp som är kopplade till organiserad brottslighet, är ett växande problem både inom unionen och på global nivå, och oron ökar för terroristattacker eller politiskt motiverade angrepp mot de informationssystem som ingår i medlemsstaternas och unionens kritiska infrastruktur. Detta utgör ett hot mot arbetet för att skapa ett säkrare informationssamhälle och ett område med frihet, säkerhet och rättvisa och kräver därför motåtgärder på unionsnivå och bättre samordning och samarbete på internationell nivå.

(2a) Inom unionen finns det en rad kritiska infrastrukturer för vilka driftstörningar eller förstörelse skulle kunna få betydande gränsöverskridande konsekvenser. Det har visat sig att behovet av att förbättra förmågan att skydda kritisk infrastruktur i unionen innebär att åtgärderna mot angrepp mot informationssystem bör kompletteras med allvarliga straffrättsliga påföljder som återspeglar angreppens svårhetsgrad. Med kritisk infrastruktur avses anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga till exempel för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, försörjningstrygghet och ekonomiska eller sociala välfärd såsom kraftverk, transportnät eller nätverk av myndigheter och där driftstörning eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner.

(3) Det finns bevis för en utveckling mot allt farligare och mer återkommande storskaliga angrepp mot informationssystem som ofta kan vara av vital betydelse för stater eller särskilda funktioner i den offentliga eller privata sektorn. Till denna tendens kommer alltmer sofistikerade metoder, såsom skapande och användning av s.k. botnät, som omfattar flera skeden i en brottslig gärning, där varje skede i sig kan utgöra ett allvarligt hot mot allmänna intressen. Direktivet syftar här bland annat till att införa straffrättsliga påföljder i det skede där botnätet skapas, då ett stort antal datorer kan tas över och fjärrstyras till följd av att de har infekterats via sabotageprogram genom riktade it-angrepp. I ett senare skede kan de smittade datorerna, som utgör botnätet, utan användarnas vetskap aktiveras för storskaliga it-angrepp, som i allmänhet kan orsaka allvarlig skada, som anges i detta direktiv. Medlemsstaterna får fastställa vad som utgör allvarlig skada enligt nationell lagstiftning och praxis, vilket bland annat kan innebära störning av systemtjänster av stort allmänintresse, orsakande av stora ekonomiska kostnader eller förlust av personuppgifter eller känslig information.

(3a) Storskaliga angrepp kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och i kommunikationen och förlust eller förvanskning av hemlig information som är viktig ur kommersiell synpunkt eller andra uppgifter. Särskild uppmärksamhet bör ägnas åt att öka medvetenheten hos innovativa små och medelstora företag om hot och svagheter, med tanke på att de i allt större utsträckning är beroende av att informationssystem fungerar korrekt och är tillgängliga, och de ofta begränsade resurser de har för informationssäkerhet.

(4) Gemensamma definitioner på detta område är viktiga för att säkerställa att detta direktiv tillämpas enhetligt i medlemsstaterna.

(5) Det finns ett behov av att fastställa en gemensam inställning i fråga om brottsrekvisit, genom att gemensamt kriminalisera olagligt intrång i informationssystem, olaglig systemstörning, olaglig datastörning och olaglig avlyssning.

(5a) Avlyssning omfattar, men är inte nödvändigtvis begränsat till, avlyssning och övervakning av kommunikationsinnehåll och framskaffande av uppgifter, antingen direkt genom åtkomst till och användning av informationssystem eller indirekt med tekniska hjälpmedel, genom användning av olika typer av elektroniska avlyssningsanordningar.

(6) Medlemsstaterna bör fastställa påföljder för angrepp mot informationssystem. De påföljder som fastställs bör vara effektiva, proportionella och avskräckande och bör inbegripa fängelsestraff och/eller ekonomiska påföljder.

(6a) I direktivet föreskrivs straffrättsliga påföljder åtminstone i fall som inte är ringa. Medlemsstaterna får fastställa vad som utgör ett ringa fall i enlighet med deras nationella lagstiftning och praxis. Ett fall kan anses vara ringa till exempel när den skada och/eller risk som gärningen medför för offentliga eller privata intressen, såsom ett datasystems eller datorbehandlingsbara uppgifters integritet eller en persons integritet, rättigheter och andra intressen, är obetydlig eller av sådan art att åläggande av straffrättsliga påföljder inom den lagstadgade gränsen eller åläggande av straffrättsligt ansvar inte är nödvändigt.

(6b) Identifiering och rapportering av hot och risker från it-angrepp och svagheter i informationssystem bör ingå i ett effektivt förebyggande av och effektiva motåtgärder mot it-angrepp och i förbättrad säkerhet för informationssystem. Effekten kan förstärkas genom incitament att rapportera säkerhetsbrister. Medlemsstaterna bör sträva efter att ge möjligheter att på ett lagligt sätt upptäcka och rapportera säkerhetsbrister.

(7) Det är lämpligt att föreskriva strängare påföljder när ett angrepp mot ett informationssystem görs inom ramen för en sådan kriminell organisation som avses i rådets rambeslut 2008/841/RIF av den 24 oktober 2008 om kampen mot organiserad brottslighet[4], eller när angreppet är storskaligt och därmed påverkar ett betydande antal informationssystem

[4] EUT L 300, 11.11.2008, s. 42.

eller orsakar avsevärd skada, inklusive när angreppet syftar till att skapa ett botnät eller genomförs via ett botnät och därmed orsakar allvarlig skada. Det är också lämpligt att föreskriva strängare påföljder när ett sådant angrepp riktas mot kritisk infrastruktur.

(7a) Införandet av effektiva åtgärder mot identitetsstöld och andra identitetsrelaterade brott utgör en annan viktig del i en samlad ansats mot it-brottslighet. Behovet av unionsåtgärder mot denna typ av brottsligt beteende kan också övervägas vid utvärderingen av behovet av ett övergripande horisontellt unionsinstrument.

(8) Enligt rådets slutsatser av den 27–28 november 2008 bör det utarbetas en ny strategi i samarbete med kommissionen och medlemsstaterna, med hänsyn till Europarådets konvention från 2001 om it-brottslighet. Konventionen är den viktigaste rättsliga referensramen när det gäller att bekämpa it-brottslighet, inklusive angrepp mot informationssystem. Detta direktiv bygger på den konventionen. Det bör därför ses som en prioritet att alla medlemsstaters ratificering av konventionen slutförs så snart som möjligt.

(9) Med hänsyn till de olika metoder som kan användas för att angripa informationssystem och till den snabba utvecklingen av hård- och programvara, hänvisar detta direktiv till verktyg som kan användas för att begå brott som förtecknas i detta direktiv. Verktyg i denna mening är exempelvis sabotageprogram, inklusive sådana som kan skapa botnät, som används för angrepp mot informationssystem. Även om ett verktyg är lämpat eller till och med särskilt lämpat för de brott som förtecknas i detta direktiv kan verktyget vara tillverkat för lagliga ändamål. Eftersom det finns ett behov av att undvika kriminalisering av fall där sådana verktyg tillverkas och saluförs för lagliga ändamål, t.ex. för test av informationsteknikprodukters funktionssäkerhet eller informationssystems säkerhet, måste, utöver det allmänna kravet på uppsåt, också ett krav på direkt uppsåt uppfyllas, att dessa verktyg är avsedda att användas för att begå något av de brott som förtecknas i detta direktiv.

(10a) Detta direktiv syftar inte till att ålägga straffrättsligt ansvar när de objektiva kriterierna för brott som förtecknas i detta direktiv är uppfyllda, men som begås utan brottsligt uppsåt, till exempel när en person inte visste att det rörde sig om obehörig åtkomst eller vid föreskrivna test eller skydd av informationssystem, dvs. när en person har fått i uppdrag av ett företag eller en leverantör att testa styrkan hos dess säkerhetssystem. Avtalsenliga skyldigheter eller överenskommelser om att begränsa åtkomst till informationssystem genom användarpolicy eller användarvillkor samt arbetsmarknadstvister om åtkomst till och användning av arbetsgivarens informationssystem för privata ändamål, bör inte föranleda straffrättsligt ansvar enligt detta direktiv, om åtkomsten under dessa omständigheter skulle bedömas vara otillåten och således utgöra den enda grunden för lagföring. Detta direktiv påverkar inte den lagligt garanterade rätten till åtkomst till information i enlighet med nationell lagstiftning och unionslagstiftning, men får samtidigt inte fungera som undantag för att motivera olaglig och godtycklig åtkomst till information.

(10b) It-angrepp kan underlättas av olika omständigheter, till exempel när förövaren i tjänsten har åtkomst till de säkerhetssystem som är inbyggda i de drabbade informationssystemen. Inom ramen för den nationella lagstiftningen bör sådana omständigheter på lämpligt sätt beaktas vid lagföring.

(10c) Medlemsstaterna bör ange försvårande omständigheter i sin nationella lagstiftning i enlighet med de tillämpliga regler om försvårande omständigheter som fastställts genom deras rättssystem. De bör se till att rätten vid lagföring kan beakta dessa försvårande omständigheter. Rätten ska göra en prövning av dessa omständigheter tillsammans med övriga omständigheter i det enskilda fallet.

(10d) Detta direktiv reglerar inte de villkor som ska vara uppfyllda för att man ska kunna utöva behörighet över något av de brott som avses i artiklarna 3–8, exempelvis att det ska föreligga en anmälan från offret på den plats där brottet begicks eller en formell underrättelse från den stat där brottet begicks, eller om det förhåller sig så att gärningsmannen inte har lagförts på den plats där gärningen har begåtts.

(10e) Stater och offentliga organ är, inom ramen för detta direktiv, skyldiga att till fullo garantera respekten för de mänskliga rättigheterna och grundläggande friheterna, i enlighet med gällande unionsförpliktelser och internationella förpliktelser.

(11) Genom detta direktiv stärks betydelsen av nätverk, såsom G8 eller Europarådets nätverk av kontaktpunkter, som är tillgängliga 24 timmar om dygnet veckans alla dagar. Sådana kontaktpunkter bör kunna ge konkret stöd och till exempel kunna underlätta utbyte av tillgänglig relevant information eller tillhandahålla teknisk rådgivning eller rättslig information i utredningar eller rättegångar rörande brott med anknytning till informationssystem och data som rör den begärande medlemsstaten. För att nätverken ska kunna fungera smidigt bör varje kontaktpunkt kunna kommunicera med kontaktpunkter i andra medlemsstater omgående, bland annat med hjälp av utbildad och utrustad personal. Med hänsyn till hur snabbt storskaliga it-angrepp kan genomföras, bör medlemsstaterna ha kapacitet att snabbt besvara brådskande förfrågningar från detta nät av kontaktpunkter. I sådana fall kan det vara lämpligt att förfrågan om information åtföljs av en telefonkontakt, för att se till att den anmodade medlemsstaten behandlar förfrågan snabbt och ger återkoppling inom åtta timmar.

(11a) Samarbete mellan de offentliga myndigheterna och den privata sektorn och det civila samhället är mycket viktigt för att förebygga och motverka angrepp mot informationssystem. Det är nödvändigt att främja och förbättra samarbetet mellan tjänsteleverantörer, producenter, brottsbekämpande organ och rättsliga myndigheter samtidigt som rättsstatsprincipen beaktas fullt ut. Samarbetet kan inbegripa t.ex. stöd från tjänsteleverantörernas sida när det gäller att säkra potentiella bevis, bidra till fastställandet av gärningsmännens identitet och, som en sista utväg, i enlighet med nationell rätt, inklusive nationell lagstiftning och rättspraxis, helt eller delvis stänga ned informationssystem eller funktioner som har angripits eller använts för olagliga ändamål. Medlemsstaterna bör också överväga att inrätta nätverk för samarbete och partnerskap med tjänsteleverantörer och producenter för utbyte av uppgifter om de brott som omfattas av detta direktiv.

(12) Det finns behov av att samla in jämförbara data om de brott som avses i detta direktiv. Relevanta data bör göras tillgängliga för behöriga specialiserade organ, t.ex. Europol och Europeiska byrån för nät- och informationssäkerhet i enlighet med deras uppdrag och informationsbehov, för att skaffa en mer heltäckande bild av problemet med it-brottslighet och nätverks- och informationssäkerhet på unionsnivå och därigenom medverka till utformningen av mer effektiva motåtgärder. Medlemsstaterna bör översända uppgifter om gärningsmännens tillvägagångssätt till Europol för utarbetande av hotbedömningar och strategiska analyser i samband med it-brottslighet i enlighet med rådets beslut 2009/371/RIF. Information kan bidra till bättre insikt om nuvarande och framtida hot och därmed bidra till att bättre och mer målinriktade beslut fattas om bekämpande och förebyggande av angrepp mot informationssystem.

(12a) I enlighet med detta direktiv ska kommissionen överlämna en rapport om tillämpningen av direktivet och lägga fram nödvändiga förslag till lagstiftning som kan leda till att detta direktivs räckvidd utvidgas med hänsyn till utvecklingen på området för it-brottslighet. Exempel på sådan utveckling är tekniska lösningar som bland annat möjliggör effektivare verkställighet på området för angrepp mot informationssystem, eller som gör det lättare att förebygga eller minimera konsekvenserna av sådana angrepp. Kommissionen bör för detta ändamål beakta tillgängliga analyser och rapporter som utarbetats av relevanta aktörer, särskilt Europol och ENISA.

(12b) För att man effektivt ska kunna bekämpa it-brottslighet är det nödvändigt att öka informationssystemens motståndskraft genom lämpliga åtgärder för att bättre skydda dem mot it-angrepp. Medlemsstaterna bör vidta nödvändiga åtgärder för att skydda kritisk infrastruktur från it-angrepp, och skyddet av deras informationssystem med tillhörande data bör ingå i det. Att se till att juridiska personer har en tillräckligt hög skydds- och säkerhetsnivå på informationssystem, t.ex. i samband med tillhandahållande av offentligt tillgängliga elektroniska kommunikationstjänster i enlighet med gällande unionslagstiftning om integritet och elektronisk kommunikation samt om dataskydd, är en viktig del i en övergripande strategi

för att effektivt motverka it-brottslighet. Lämpliga skyddsnivåer bör tillhandahållas mot hot och svagheter som rimligen kan identifieras i enlighet med den senaste utvecklingen inom den specifika sektorn och de konkreta situationerna för databehandlingen. De kostnader och bördor som ett sådant skydd medför bör stå i förhållande till den sannolika skadan av ett it-angrepp för de drabbade. Medlemsstaterna uppmanas att fastställa relevanta åtgärder i fråga om ansvar inom ramen för nationell lagstiftning när det är uppenbart att en juridisk person inte har haft en lämplig skyddsnivå mot it-angrepp.

(13) Stora klyftor och skillnader i medlemsstaternas lagstiftning och straffrättsliga förfaranden på detta område kan försvåra kampen mot organiserad brottslighet och terrorism, och komplicera ett effektivt polisiärt och rättsligt samarbete när det gäller angrepp mot informationssystem. De moderna informationssystemens nationsöverskridande och gränslösa natur innebär att angrepp mot sådana system ofta har en gränsöverskridande dimension, vilket understryker det trängande behovet av ytterligare insatser för att tillnärma den straffrättsliga lagstiftningen på detta område. För övrigt torde adekvata åtgärder för genomförande och tillämpning av rådets rambeslut 2009/948/RIF om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden göra det lättare att samordna lagföringen av angrepp mot informationssystem. Medlemsstaterna bör också i samarbete med Europeiska unionen verka för bättre internationellt samarbete i fråga om säkerheten i informationssystem, datornätverk och datorbehandlingsbara uppgifter. Vederbörlig hänsyn till säkerheten vid dataöverföring och lagring av uppgifter bör tas med i alla internationella avtal som rör uppgiftsutbyte.

(13a) Bättre samarbete mellan behöriga brottsbekämpande organ och rättsliga myndigheter i hela unionen är nödvändigt för att man ska kunna bekämpa it-brottslighet på ett effektivt sätt. I detta sammanhang bör ökade insatser för att ge adekvat utbildning till de berörda myndigheterna för ökad förståelse av it-brottslighet och dess konsekvenser, och för att främja samarbete och utbyte av bästa metoder, exempelvis genom de behöriga specialiserade unionsorganen, uppmuntras. Sådan utbildning bör bland annat syfta till att öka medvetenheten om

de olika nationella rättssystemen, de rättsliga och tekniska svårigheter som kan uppstå vid brottsutredningar eller fördelningen av befogenheter mellan de relevanta nationella myndigheterna.

(14) Eftersom målen för detta direktiv, nämligen att säkerställa att angrepp mot informationssystem i alla medlemsstater bestraffas med effektiva, proportionella och avskräckande straffrättsliga påföljder och att förbättra och uppmuntra rättsligt samarbete genom att undanröja eventuella komplikationer, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, och de därför bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(15a) Skyddet av personuppgifter är en grundläggande rättighet i enlighet med artikel 16.1 i EUF-fördraget och artikel 8 i stadgan om de grundläggande rättigheterna. Därför bör all behandling av personuppgifter i samband med genomförandet av detta direktiv vara helt och hållet förenlig med tillämplig unionslagstiftning om uppgiftsskydd som antagits på grundval av fördragen.

(16) Detta direktiv står i överensstämmelse med grundläggande friheter och rättigheter och de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, inklusive skyddet av personuppgifter, rätten till integritet, yttrande- och informationsfrihet, rätten till en rättvis rättegång, oskuldspresumtion och rätten till försvar, samt med legalitetsprincipen och principen om proportionalitet mellan brottet och påföljden. Detta direktiv syftar särskilt till att sörja för att dessa rättigheter och principer respekteras fullt ut och måste genomföras i enlighet med detta.

(17) I enlighet med artikel 3 i protokollet om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska

unionens funktionssätt, har dessa medlemsstater meddelat att de önskar delta i antagandet och tillämpningen av detta direktiv.

(18) I enlighet med artiklarna 1 och 2 i protokollet om Danmarks ställning, fogat till fördraget om Europeiska unionens funktionssätt, deltar Danmark inte i antagandet av detta direktiv, som därför inte är bindande för eller tillämpligt i förhållande till Danmark.

(19) Syftet med detta direktiv är att ändra och utöka bestämmelserna i rambeslut 2005/222/RIF. Med avseende på de medlemsstater som deltar i antagandet av detta direktiv bör rambeslutet för tydlighetens skull ersättas i sin helhet, eftersom de ändringar som görs är många och väsentliga.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1
Syfte

Detta direktiv fastställer minimiregler om fastställande av brottsrekvisit och påföljder inom området angrepp mot informationssystem. Det syftar också till att främja förebyggande av sådana brott och förbättra samarbetet mellan rättsliga och andra behöriga myndigheter.

Artikel 2
Definitioner

I detta direktiv avses med

a) *informationssystem*: en apparat eller en grupp av sammankopplade apparater eller 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 ska kunna drivas, användas, skyddas och underhållas,

b) *datorbehandlingsbara uppgifter*: 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,

c) *juridisk person*: enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer,

d) *orättmätigt*: intrång, störning, avlyssning eller något annat handlande som avses i detta direktiv, som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta, eller som inte medges i den nationella lagstiftningen.

Artikel 3
Olagligt intrång i informationssystem

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att orättmätigt intrång som begås med uppsåt i ett informationssystem som helhet eller en del av ett sådant system straffbeläggs när brottet begås genom intrång i en säkerhetsåtgärd, åtminstone i fall som inte är ringa.

Artikel 4
Olaglig systemstörning

Medlemsstaterna ska vidta nödvändiga åtgärder för att se till att det är straffbart att 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, när gärningen begås med uppsåt och orättmätigt, åtminstone i fall som inte är ringa.

Artikel 5
Olaglig datastörning

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det är straffbart att radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, när gärningen begås med uppsåt och orättmätigt, åtminstone i fall som inte är ringa.

Artikel 6
Olaglig avlyssning

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att avlyssning med tekniska hjälpmedel av icke-offentliga överföringar av datorbehandlingsbara uppgifter till, från eller inom ett informationssystem, inklusive elektromagnetisk strålning från informationssystem som innehåller sådana uppgifter, straffbeläggs när gärningen begås med uppsåt och orättmätigt, åtminstone i fall som inte är ringa.

Artikel 7
Verktyg som används för att begå brott

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det är straffbart att tillverka, sälja, anskaffa i syfte att använda, importera, distribuera eller på annat sätt tillgängliggöra följande verktyg, om gärningen begås med uppsåt och orättmätigt, i syfte att begå något av de brott som avses i artiklarna 3–6, åtminstone i fall som inte är ringa:

a) Ett datorprogram som utformats eller anpassats i första hand för att begå något av de brott som avses i artiklarna 3–6,

b) Ett lösenord, en åtkomstkod eller liknande uppgifter som gör det möjligt att få tillgång till ett informationssystem eller delar av ett sådant system.

Artikel 8
Anstiftan, medhjälp och försök

1. Medlemsstaterna ska se till att anstiftan av och medhjälp till de brott som avses i artiklarna 3–7 straffbeläggs.

2. Medlemsstaterna ska se till att försök att begå de brott som avses i artiklarna 4–5 straffbeläggs.

Artikel 9
Påföljder

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–8 är belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–7 är belagda med ett maximistraff på minst två års fängelse, åtminstone i fall som inte är ringa.

3. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 4–5 är belagda med ett maximistraff på minst tre års fängelse när de begås med uppsåt, när ett betydande antal informationssystem har påverkats genom användning av ett verktyg som avses i artikel 7, utformat eller anpassat i första hand för detta syfte.

4. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 4–5 är belagda med ett maximistraff på minst fem års fängelse när de

   a) begås inom ramen för en kriminell organisation enligt definitionen i rambeslut 2008/814/RIF, oberoende av den påföljdsnivå som anges där, eller

   b) förorsakar allvarlig skada, eller

   c) begås mot ett kritiskt informationsinfrastruktursystem.

5. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det i enlighet med tillämpliga bestämmelser i nationell lag kan anses som en försvårande omständighet när de brott som avses i artiklarna 4 och 5 begås genom missbruk av personuppgifter som rör en annan person än gärningsmannen, i syfte att vinna tredje mans förtroende, och därigenom medför skada för den som identiteten tillhör, om inte dessa omständigheter redan täcks av ett annat brott som är straffbart enligt nationell lagstiftning.

Artikel 11
Juridiska personers ansvar

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar för de brott som avses i artiklarna 3–8 och som begås till deras förmån av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom den juridiska personen, grundad på något av följande:

   a) Behörighet att företräda den juridiska personen.

   b) Befogenhet att fatta beslut på den juridiska personens vägnar.

   c) Befogenhet att utöva kontroll inom den juridiska personen.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar när brister i övervakning eller kontroll som ska utföras av en sådan person som avses i punkt 1 har gjort det möjligt för en person som är underställd den juridiska personen att till förmån för denna juridiska person begå något av de brott som avses i artiklarna 3–8.

3. Juridiska personers ansvar enligt punkterna 1 och 2 ska inte utesluta lagföring av fysiska personer som begår, anstiftar eller medverkar till något av de brott som avses i artiklarna 3–8.

Artikel 12
Påföljder för juridiska personer

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 11.1 kan bli föremål för effektiva, proportionella och avskräckande påföljder, som ska innefatta bötesstraff eller administrativa avgifter och som får innefatta andra sanktioner, som

   a) att rätten till offentliga förmåner eller stöd dras in,

   b) tillfälligt eller permanent näringsförbud,

   c) rättslig övervakning,

   d) rättsligt beslut om upplösning av verksamheten,

e) tillfällig eller permanent stängning av inrättningar som har använts för att begå brottet.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 11.2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller åtgärder.

Artikel 13
Behörighet

1. Medlemsstaterna ska fastställa sin behörighet beträffande de brott som avses i artiklarna 3–8, när brottet har begåtts

   a) helt eller delvis på en medlemsstatsterritorium, eller

   b) av en medborgare i medlemsstaten, åtminstone i sådana fall där gärningen utgör ett brott på den plats där den begicks.

2. En medlemsstat ska vid fastställandet av sin behörighet enligt punkt 1 a se till att behörigheten innefattar fall där

   a) gärningsmannen är fysiskt närvarande på dess territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på denna medlemsstats territorium eller inte, eller

   b) brottet riktar sig mot ett informationssystem på dess territorium, oavsett om gärningsmannen är fysiskt närvarande på detta territorium när brottet begås eller inte.

3. En medlemsstat ska underrätta kommissionen om den beslutar att fastställa ytterligare behörighet över ett brott enligt artikel 3–8 som har begåtts utanför dess territorium, t.ex. när

   a) gärningsmannen har sin hemvist på denna medlemsstats territorium, eller

   b) gärningen har begåtts till förmån för en juridisk person som är etablerad inom denna medlemsstats territorium.

Artikel 14
Informationsutbyte

1. För utbyte av uppgifter om de brott som avses i artiklarna 3–8 ska medlemsstaterna se till att ha en operativ nationell kontaktpunkt och använda det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan. Medlemsstaterna ska också se till att ha förfaranden som gör att de vid brådskande förfrågningar inom högst åtta timmar efter mottagandet kan ange åtminstone huruvida framställningen om bistånd kommer att besvaras samt formen och den beräknade tidpunkten för svaret.

2. Medlemsstaterna ska underrätta kommissionen om sin utsedda kontaktpunkt för utbyte av uppgifter om de brott som avses i artiklarna 3–8. Kommissionen ska vidarebefordra denna information till de andra medlemsstaterna och behöriga specialiserade unionsorgan och byråer.

3. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att lämpliga rapporteringskanaler är tillgängliga för att underlätta att de brott som avses i artiklarna 3–6 rapporteras till behöriga nationella myndigheter utan onödigt dröjsmål.

Artikel 15
Övervakning och statistik

1. Medlemsstaterna ska se till att det finns ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om de brott som avses i artiklarna 3–7.

2. De statistiska uppgifter som avses i punkt 1 ska åtminstone omfatta befintliga uppgifter om antalet sådana brott som avses i artiklarna 3–7 som registrerats av medlemsstaterna och antalet personer som åtalats och dömts för sådana brott som avses i artiklarna 3–7.

3. Medlemsstaterna ska översända de uppgifter som samlas in enligt denna artikel till kommissionen. Kommissionen ska se till att en samlad översikt över dessa statistiska rapporter offent-

liggörs och översänds till behöriga specialiserade unionsorgan och byråer.

Artikel 16
Ersättande av rambeslut 2005/222/RIF

Rambeslut 2005/222/RIF ersätts härmed med avseende på de medlemsstater som deltar i antagandet av detta direktiv, dock utan att det påverkar medlemsstaternas skyldigheter när det gäller tidsfristen för införlivande i nationell lagstiftning av rambeslutet.

Med avseende på de medlemsstater som deltar i antagandet av detta direktiv ska hänvisningar till rambeslut 2005/222/RIF anses som hänvisningar till detta direktiv.

Artikel 17
Införlivande

1. Medlemsstaterna ska senast [två år efter antagandet] sätta i kraft de lagar och andra författningar som är nödvändiga för att följa detta direktiv.

2. Medlemsstaterna ska till kommissionen överlämna texten till de bestämmelser genom vilka skyldigheterna enligt detta direktiv införlivas med deras nationella lagstiftning.

3. När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 18
Rapportering

Kommissionen ska senast [fyra år efter antagandet] överlämna en rapport till Europaparlamentet och rådet med en utvärdering av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa bestämmelserna i detta direktiv, vid behov åtföljd av lagstiftningsförslag. Kommissionen ska därvid även beakta den tekniska och rättsliga utvecklingen på området för itbrottslighet, särskilt vad gäller tillämpningsområdet för detta direktiv.

Artikel 19
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i Europeiska unionens officiella tidning.

Artikel 20
Adressater

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

Statens offentliga utredningar 2013

Kronologisk förteckning

1. Förändrad hantering av importmoms. Fi.
2. Patientlag. S.
3. Trängselskatt – delegation, sanktioner och utländska fordon. Fi.
4. Tillstånd och medling. Ju.
5. Djurhållning och miljön
   – hantering av risker och möjligheter med stallgödsel. L.
6. Att förebygga och hantera finansiella kriser. Fi.
7. Skärpningar i vapenlagstiftningen. Ju.
8. Den svenska veteranpolitiken
   Statligt bidrag till frivilliga organisationer som stödjer veteransoldater och anhöriga. Fö.
9. Riksbankens
   finansiella oberoende och balansräkning. Fi.
10. Rätta byggfelen snabbt!
    – med effektivare förelägganden och försäkringar. S.
11. Kunskapsläget på Kärnavfallsområdet 2013. Slutförvarsansökan under prövning: kompletteringskrav och framtidsalternativ. M.
12. Goda affärer – en strategi för hållbar, offentlig upphandling. Fi.
13. Ungdomar utanför gymnasieskolan
    – ett förtydligat ansvar för stat och kommun. U.
14. En översyn inom Sevesoområdet
    – förslag till en förstärkt organisation för att förebygga och begränsa följderna av allvarliga kemikalieolyckor. Fö.
15. För framtidens hälsa –
    en ny läkarutbildning. U.
16. Effektivare konkurrenstillsyn. N.
17. Brottmålsprocessen. Del 1 och 2. Ju.
18. Regeringsbeslut av ett statsråd – SRÄ. Fö.
19. Mera glädje för pengarna. Ku.
20. Kommunal vuxenutbildning på grundläggande nivå – en översyn för ökad individanpassning och effektivitet. U.
21. Internationell straffverkställighet. Ju.
22. Så enkelt som möjligt för så många som möjligt
    – samordning och digital samverkan. N.
23. Ersättning vid läkemedelsskador och miljöhänsyn i läkemedelsförmånerna. S.
24. E-röstning och andra valfrågor. Ju.
25. Åtgärder för ett längre arbetsliv. +Lättläst + Daisy. S.
26. Fri att leka och lära
    – ett målinriktat arbete för barns ökade säkerhet i förskolan. U.
27. Vissa frågor om gode män och förvaltare. Ju.
28. Försäkring på transportområdet i krig och kris. Fi.
29. Det svenska medborgarskapet. A.
30. Det tar tid
    – om effekter av skolpolitiska reformer. U.
31. En digital agenda i människans tjänst
    – Sveriges digitala ekosystem, dess aktörer och drivkrafter. N.
32. Budgetramverket
    – uppfyller det EU:s direktiv? Fi.
33. En myndighet för alarmering. Fö.
34. En effektivare plan- och bygglovsprocess. S.
35. En ny lag om personnamn. Ju.
36. Disciplinansvar i ett reformerat försvar. Fö.
37. Begripliga beslut på migrationsområdet. Ju.
38. Vad bör straffas? Del 1 och 2. Ju.
39. Europarådets konvention om it-relaterad brottslighet. Ju.

Statens offentliga utredningar 2013

Systematisk förteckning

En digital agenda i människans tjänst
– Sveriges digitala ekosystem, dess aktörer och drivkrafter. [31]

Kulturdepartementet

Mera glädje för pengarna. [19]

Arbetsmarknadsdepartementet

Det svenska medborgarskapet. [29]