Lagrådsremiss

Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 19 november 2020

Morgan Johansson

Frida Göranson
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Regeringen föreslår att Sverige ska tillträda Europarådets konvention om it-relaterad brottslighet och dess tilläggsprotokoll. Konventionens huvudsakliga syfte är att harmonisera konventionsstaternas nationella lagstiftningar som rör it-relaterad brottslighet och att förenkla det internationella samarbetet kring dessa frågor.

Regeringen lämnar förslag på de lagändringar som behövs för ett tillträde. Förslagen innebär bl.a. att den som innehar en viss lagrad elektronisk uppgift som behövs i en brottsutredning ska kunna föreläggas att bevara uppgiften, en form av s.k. frysning. Förslagen innebär ingen utökad skyldighet att införskaffa eller lagra elektronisk information i förväg. Det innebär inte heller några utökade möjligheter att få informationen utlämnad. Det föreslås vidare en skyldighet för den som tillhandahåller elektroniska kommunikationsnät och tjänster att lämna ut information om vilka som har deltagit vid överföringen av ett meddelande. De åtgärder som införs ska även kunna användas i det internationella straffrättsliga samarbetet.

Lagändringarna föreslås träda i kraft den 1 maj 2021.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om ändring i rättegångsbalken,
2. lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål,
3. lag om ändring i lagen (2003:389) om elektronisk kommunikation,
4. lag om ändring i lagen (2017:1000) om en europeisk utredningsorder.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att det i rättegångsbalken ska införas två nya paragrafer, 27 kap. 16 och 16 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 det anges hur länge uppgiften ska bevaras. Tiden får inte bestämmas till längre än nödvändigt och får inte överstiga 90 dagar från dagen för beslutet.
	Om det finns särskilda skäl får tiden för bevarande förlängas med högst 90 dagar.
	Ett föreläggande får inte riktas mot den som skäligen kan misstänkas för brottet eller mot någon till honom eller henne sådan närstående person som avses i 36 kap. 3 §.
	16 a §
	Ett föreläggande enligt 16 § får beslutas av undersökningsledaren eller en åklagare.
	I föreläggandet får det anges att den som har förelagts att bevara en viss uppgift inte får uppenbara att åtgärden har vidtagits.
	Den som har förelagts att bevara en viss uppgift får begära rättens prövning av föreläggandet. För rättens prövning gäller 6 § första stycket.

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

Denna lag träder i kraft den 1 maj 2021.

2.2 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 § och 2 kap. 1 och 2 §§ ska ha följande lydelse,

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

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[1]	
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 att bevara en viss lagrad uppgift 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. hemlig kameraövervakning,	*8*. hemlig kameraövervakning,
8. hemlig rumsavlyssning,	*9*. hemlig rumsavlyssning,
9. hemlig dataavläsning,	*10*. hemlig dataavläsning,
10. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,	*11*. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,
11. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,	*12*. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,
12. överförande av frihetsberövade för förhör m.m., och	*13*. överförande av frihetsberövade för förhör m.m., och

[1] Senaste lydelse 2020:65.

13. rättsmedicinsk undersökning av en avliden person.	*14*. rättsmedicinsk undersökning av en avliden person.

Lagen hindrar inte att hjälp lämnas med någon 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 §[2]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–*9* 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 1–*10* och *14* 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 *10–12* lämnas enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *11–13* 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 §[3]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *10* 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–*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.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *6, 11* och *13* 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, 7–10*, *12* och *14* 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.

[2] Senaste lydelse 2020:65.
[3] Senaste lydelse 2020:65.

4 kap.

Föreläggande att bevara en viss lagrad uppgift

24 c §

En ansökan om ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken handläggs av en åklagare.

Denna lag träder i kraft den 1 maj 2021.

2.3 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. 8, 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.	
8 §[1]	
Bestämmelserna i 5–7 §§ gäller inte	
1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 5 § för att lösa tvister,	
	2. för elektroniska meddelanden som omfattas av ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,
2. för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, eller	*3.* för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, eller
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	*4.* i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.
16 c §[2]	
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	Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 *eller 14*, 27 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om

[1] Senaste lydelse 2012:285.

[2] Senaste lydelse 2012:285.

kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

16 d §[3]

Uppgifter som avses i 16 a § ska lagras enligt följande:

– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock lagras i endast två månader.

– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de dock lagras i endast sex månader.

Lagringstiden räknas från den dag kommunikationen avslutades.

När lagringstiden löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande har kommit in innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de lämnats ut. *Efter utlämnandet* ska uppgifterna genast utplånas.

När lagringstiden *har* löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande har kommit in *eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har meddelats* innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de *har* lämnats ut *eller tiden för bevarande har löpt ut*. *Därefter* ska uppgifterna genast utplånas.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om lagringstiden enligt första stycket.

16 g §

Om någon som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § har förelagts att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken gäller 3 a, 16 e och 16 f §§ på motsvarande sätt för den uppgift som ska bevaras.

21 §[4]

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

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

[3] Senaste lydelse 2019:497.
[4] Senaste lydelse 2012:285.

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*	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.	5. begäran om utlämnande av uppgift om abonnemang enligt 22 § första stycket 2*,*
	6. föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken, och
	7. begäran om utlämnande av en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster enligt 22 § första stycket 14.

22 §[5]

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 en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen 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 Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns 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

[5] Senaste lydelse 2020:340.

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 Polismyndigheten, 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 Polismyndigheten eller en 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,

9. uppgift som avses i 20 § första stycket 1 till Finansinspektionen, om inspektionen finner att uppgiften är av väsentlig betydelse för utredningen av en misstänkt överträdelse av Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentet och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG,

10. uppgift som avses i 20 § första stycket 1 till Finansinspektionen, om inspektionen finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller någon av bestämmelserna i 4 a kap. 1–8 §§ lagen (2010:751) om betaltjänster eller 1 kap. 5 § eller 4 kap. 7, 8, 9, 10, 11 eller 14 § lagen (2016:1024) om verksamhet med bostadskrediter,

11. uppgift som avses i 20 § första stycket 1 till Konsumentombudsmannen, om ombudsmannen finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden eller marknadsföringslagen (2008:486), när det är fråga om en misstänkt överträdelse av unionslagstiftning som skyddar konsumenternas intressen enligt bilagan till Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004,

12. uppgift som avses i 20 § första stycket 1 till Läkemedelsverket, om verket finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i 12 kap. läkemedelslagen (2015:315), *och*

13. uppgift som avses i 20 § första stycket 1 till Konsumentverket, om verket finner att uppgiften

12. uppgift som avses i 20 § första stycket 1 till Läkemedelsverket, om verket finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i 12 kap. läkemedelslagen (2015:315),

13. uppgift som avses i 20 § första stycket 1 till Konsumentverket, om verket finner att uppgiften

är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning.	är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning*, och*
	14. uppgift som avses i 20 § första stycket 3 om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § 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 maj 2021.

2.4 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 3 kap. 5 § och 4 kap. 1 och 2 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 2 kap. 16 a § och 3 kap. 33 a §, och närmast före 2 kap. 16 a § och 3 kap. 33 a § nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

1 kap.

4 §[1]

En utredningsåtgärd enligt denna lag ska avse eller motsvara

1. förhör under förundersökning,
2. bevisupptagning vid domstol,
3. förhör genom ljudöverföring eller ljud- och bildöverföring,

4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken *eller* en åtgärd enligt 27 kap. 15 § samma balk,	4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § *eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 §* samma balk,

5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,
7. tillfälligt överförande av en frihetsberövad person,
8. rättsmedicinsk undersökning av en avliden person,
9. kontrollerad leverans,
10. bistånd i en brottsutredning med användning av en skyddsidentitet,
11. inhämtande av bevis som finns hos en myndighet, eller
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.

2 kap.

Föreläggande att bevara en viss lagrad uppgift

16 a §

När en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har verkställts i

[1] Senaste lydelse 2020:67.

den andra medlemsstaten får den som har förelagts åtgärden begära rättens prövning. För rättens prövning gäller 27 kap. 6 § första stycket samma balk.

Den tid en uppgift enligt 27 kap. 16 § andra stycket rättegångsbalken ska bevaras, räknas från den tidpunkt då åtgärden verkställdes i den andra medlemsstaten. Om det finns särskilda skäl får tiden för bevarande förlängas med högst 90 dagar.

3 kap.

5 §

En utredningsorder får inte erkännas och verkställas i Sverige om

1. det skulle strida mot bestämmelser om immunitet och privilegier eller om skydd för uppgifter som avses i 36 kap. 5 och 5 a §§ rättegångsbalken,

2. ordern avser beslag av en skriftlig handling eller ett skriftligt meddelande och det enligt 27 kap. 2 § rättegångsbalken finns hinder mot att ta handlingen eller meddelandet i beslag,

2. ordern avser beslag av en skriftlig handling eller ett skriftligt meddelande *eller ett föreläggande att bevara en viss lagrad uppgift* och det enligt 27 kap. 2 § rättegångsbalken finns hinder mot att ta handlingen eller meddelandet i beslag *eller enligt 27 kap. 16 § fjärde stycket samma balk meddela ett föreläggande*,

3. det skulle medföra fara för Sveriges säkerhet, äventyra enskilda personers säkerhet eller medföra risk för röjande av uppgifter som rör underrättelseverksamhet,

4. den gärning som avses i utredningsordern har begåtts utanför den utfärdande medlemsstatens territorium och helt eller delvis i Sverige, och gärningen inte motsvarar ett brott enligt svensk lag, eller

5. utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 §.

En utredningsorder får inte vägras enligt första stycket 5, om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser.

Föreläggande att bevara en viss lagrad uppgift

33 a §

När en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har verkställts, tillämpas 32 § första, fjärde och femte styckena.

4 kap.

1 §

Domstolens beslut enligt 2 kap. 5, 14 *och* 16 §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *angående* den åtgärd som avses i utredningsordern.	Domstolens beslut enligt 2 kap. 5, 14*,* 16 *och 16 a* §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *om* den åtgärd som avses i utredningsordern.

Ett beslut i fråga om att utfärda en utredningsorder får inte överklagas.

2 §

Domstolens beslut enligt 3 kap. 9, 32 *och* 33 §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *angående* en åtgärd som motsvarar den åtgärd som avses i utredningsordern. Domstolens beslut enligt 3 kap. 25 § får överklagas på det sätt som gäller enligt rättegångsbalken.	Domstolens beslut enligt 3 kap. 9, 32*,* 33 *och 33 a* §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *om* en åtgärd som motsvarar den åtgärd som avses i utredningsordern. Domstolens beslut enligt 3 kap. 25 § får överklagas på det sätt som gäller enligt rättegångsbalken.

Övriga beslut i fråga om erkännande och verkställighet av en utredningsorder får inte överklagas.

Denna lag träder i kraft den 1 maj 2021.

3 Ärendet och dess beredning

Sverige undertecknade Europarådets konvention om it-relaterad brottslighet (kallad Budapestkonventionen) den 23 november 2001 och tilläggsprotokollet till konventionen den 28 januari 2003. Konventionen och tilläggsprotokollet i den officiella engelska lydelsen och svensk översättning finns i *bilagorna 1* och *2*.

Frågan om Sverige bör tillträda Budapestkonventionen och tilläggsprotokollet samt vilka lagändringar som krävs för ett tillträde behandlades i departementspromemorian Brott och brottsutredning i it-miljö (Ds 2005:6). En sammanfattning av promemorian i relevanta delar finns i *bilaga 3*. Departementspromemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2005/02234). I lagrådsremissen behandlar regeringen promemorians förslag att Sverige ska tillträda Budapestkonventionen och tilläggsprotokollet.

Efter att promemorian hade remitterats kom förutsättningarna för bedömningen av om svensk rätt uppfyller konventionens krav väsentligen att förändras genom ett antal lagstiftningsärenden på området. Regeringen beslutade därför den 27 oktober 2011 att ge en särskild utredare i uppdrag att på nytt analysera behovet av och lämna förslag på de författningsändringar som krävs för att Sverige ska kunna tillträda konventionen och tilläggsprotokollet (dir. 2011:98).

Utredningen överlämnade i maj 2013 betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39). En sammanfattning av betänkandet i relevanta delar finns i *bilaga 5*. Utredningens lagförslag i relevanta delar finns i *bilaga 6*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 7*. En sammanställning av remissyttrandena i ärendet finns tillgänglig i Justitiedepartementet (Ju2013/04173). I lagrådsremissen behandlar regeringen utredningens förslag som rör genomförandet av Budapestkonventionen i svensk rätt. De delar av betänkandet som rör Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF har behandlats i propositionen Skärpt straff för dataintrång (prop. 2013/14:92).

Sedan betänkandet remitterades har lagen (2017:1000) om en europeisk utredningsorder införts. I promemorian Kompletterande förslag inför ett tillträde till Budapestkonventionen lämnas förslag på vilka ändringar som behöver göras i den lagen bl.a. i anledning av det nya tvångsmedel som föreslagits av utredningen. En sammanfattning av promemorian i relevanta delar finns i *bilaga 8*. Promemorians lagförslag finns i *bilaga 9*. Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 10*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2020/01688).

4 Budapestkonventionen och tilläggsprotokollet

Dagens samhälle präglas av att informationsteknik genomsyrar i stort sett alla sektorer. 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. Budapestkonventionen har utarbetats för att tillgodose det behovet.

I november 1996 beslutade Europarådets straffrättsliga styrkommitté (CDPC) att uppdra åt en expertkommitté att utreda frågor rörande it-relaterad brottslighet. Efter beslut i ministerrådet påbörjades arbetet med en konvention om it-relaterad brottslighet i april 1997. Konventionen antogs av ministerrådet och öppnades för undertecknande 2001. Den trädde i kraft den 1 juli 2004. Hittills har 68 stater undertecknat konventionen och 65 stater ratificerat den, bland dem den absoluta majoriteten av EU:s medlemsstater och de övriga nordiska länderna.

Budapestkonventionen 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 behovet 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 är indelad i fyra kapitel. Dessa innehåller definitioner (kapitel I), bestämmelser om straff- och processrättsliga åtgärder som ska vidtas på nationell nivå (kapitel II), bestämmelser om internationellt samarbete (kapitel III) och slutbestämmelser (kapitel IV).

I kapitel II är bestämmelserna uppdelade i tre avsnitt. Bestämmelserna i avsnitt 1 ställer krav på kriminalisering av vissa gärningar som begås med hjälp av ett datorsystem. De processrättsliga reglerna finns i avsnitt 2. Där ställs krav på att medlemsstaterna ska kunna vidta olika former av åtgärder vid utredningen av de brott som omfattas av konventionen. I avsnitt 3 finns regler om domsrätt.

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

Ett tilläggsprotokoll öppnades för undertecknande i januari 2003 och trädde i kraft den 1 mars 2006. Tilläggsprotokollet kriminaliserar gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem. Hittills har 45 stater undertecknat tilläggsprotokollet och 32 stater ratificerat det. Tilläggsprotokollet är uppbyggt på samma sätt som konventionen. Det innehåller gemensamma bestämmelser (kapitel I), bestämmelser om straffrättsliga åtgärder (kapitel II), bestämmelser om

förhållandet mellan konventionen och tilläggsprotokollet (kapitel III) samt slutbestämmelser (kapitel IV).

Bestämmelserna i kapitel II ställer krav på kriminalisering av vissa gärningar av rasistisk och främlingsfientlig natur som begås med hjälp av ett datorsystem. Tillämpningsområdet för konventionens processrättsliga bestämmelser och bestämmelser om internationellt samarbete utvidgas också till att gälla brott som omfattas av tilläggsprotokollet, vilket framgår av kapitel III.

Mot bakgrund av den snabba teknikutvecklingen och inte minst den ökade användningen av s.k. molntjänster inleddes 2017 ett arbete med att ta fram ett andra tilläggsprotokoll till konventionen. I det arbetet ska bl.a. övervägas hur det rättsliga samarbetet kan effektiviseras ytterligare och om det finns behov av ett direktsamarbete med tjänsteleverantörer i en annan jurisdiktion för utlämnande av data i vissa situationer. Arbetet med protokollet beräknas vara klart i december 2020.

5 Sverige ska tillträda Budapestkonventionen

Regeringens förslag: Riksdagen godkänner att Sverige tillträder Budapestkonventionen och tilläggsprotokollet.

Departementspromemorians förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget.

Skälen för regeringens förslag: 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 dessvärre en tydlig baksida och har medfört nya möjligheter att begå brott utan att gärningsmannen befinner sig i det land där brottet får effekt. Det har också skapats nya 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 it-relaterade brott kan bara utredas om 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 än mer aktivt i det samarbetet.

Det är samtidigt viktigt att värna om grundläggande värden, normer och principer för den svenska rättsstaten. Särskilt viktigt i sammanhanget är upprätthållandet av de mänskliga rättigheterna, inte minst yttrandefriheten och informationsfriheten. Rätten till skydd för den personliga integriteten och värnandet om den enskildes rättssäkerhet är andra viktiga värden.

Budapestkonventionen och tilläggsprotokollet har tillkommit i syfte att effektivisera det internationella samarbetet mot it-relaterad brottslighet. I departementspromemorian Brott och brottsutredning i it-miljö (Ds 2005:6) görs bedömningen att Sverige bör tillträda såväl Budapestkonventionen som tilläggsprotokollet. Promemorian har remissbehandlats och samtliga remissinstanser som yttrar sig i frågan är positiva till att konventionen och tilläggsprotokollet tillträds.

Det finns starka skäl för Sverige att delta aktivt i det internationella samarbetet mot it-brottslighet, inte minst för att kunna utreda och lagföra allvarliga brott som t.ex. it-relaterade barnpornografibrott. Regeringen anser att Sverige bör ratificera Budapestkonventionen och tilläggsprotokollet. Eftersom ett tillträde medför lagändringar krävs riksdagens godkännande (se 10 kap. 3 § regeringsformen). Regeringen föreslår att riksdagen godkänner att Sverige tillträder Budapestkonventionen och tilläggsprotokollet.

Budapestkonventionen innehåller krav på att konventionsstaterna kriminaliserar vissa gärningar. Konventionen innehåller också krav på att staterna inför en möjlighet att vidta vissa processrättsliga åtgärder och lämnar internationell rättslig hjälp med sådana åtgärder vid utredningen av dessa brott. Konventionsstaterna har också möjlighet att lämna reservationer och förbehåll i begränsade delar om det krävs på grund av den nationella rättsordningen. Konventionens bestämmelser bör i likhet med andra överenskommelser av liknande slag omarbetas till svensk författningstext. Om svensk rätt redan uppfyller konventionens krav behövs inga författningsändringar. Utredningens bedömning är att svensk rätt redan uppfyller konventionens krav på straffrättsliga bestämmelser fullt ut men att lagändringar är nödvändiga för att uppfylla kraven i den processrättsliga regleringen och i bestämmelserna om internationellt samarbete. Behovet av och i förekommande fall förslag till lagändringar behandlas i avsnitt 6.1–6.3.

Sverige lämnade inga förbehåll vid undertecknandet av konventionen eller tilläggsprotokollet. Möjligheten att göra det kvarstår emellertid fram till ratificeringen. Behovet av förbehåll tas upp i avsnitt 6.4.

De artiklar i konventionen och tilläggsprotokollet som regeringen bedömer att svensk rätt redan uppfyller behandlas i avsnitt 7–8.

6 Behovet av lagändringar och förbehåll

6.1 Skyndsamt säkrande av lagrade uppgifter (artikel 16 och 29)

6.1.1 En möjlighet till frysning av uppgifter införs

Regeringens 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 det anges under hur lång tid uppgiften ska bevaras. Tiden får inte bestämmas till längre än nödvändigt och får inte överstiga 90 dagar från dagen

för beslutet. Om det finns särskilda skäl får tiden förlängas med högst 90 dagar.

Ett föreläggande får inte riktas mot den som skäligen kan misstänkas för brott eller mot någon till honom eller henne närstående.

I föreläggandet får det anges att den som har förelagts att bevara en viss uppgift inte får uppenbara att åtgärden har vidtagits. Den som förelagts att bevara en viss uppgift får begära rättens prövning av åtgärden. Rätten ska pröva frågan skyndsamt.

Om ett föreläggande riktas mot en sådan tjänsteleverantör som omfattas av lagen (2003:389) om elektronisk kommunikation ska vissa bestämmelser i den lagen om bl.a. ersättning och tystnadsplikt gälla.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att tiden för bevarande ska få förlängas med högst 30 dagar.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Bahnhof AB*, *Post- och telestyrelsen, Stiftelsen för Internetinfrastruktur (Internetstiftelsen)* och *Sveriges advokatsamfund* avstyrker helt eller delvis förslaget. *Ekobrottsmyndigheten*, *Polismyndigheten* och *Säkerhetspolisen* understryker att möjligheten till föreläggande om bevarande är ett efterlängtat verktyg som länge efterfrågats inom brottsbekämpningen. *Bahnhof AB, Datainspektionen, Justitiekanslern (JK), Post- och telestyrelsen, Riksdagens ombudsmän (JO), Internetstiftelsen* och *Sveriges advokatsamfund* lämnar synpunkter avseende balansen mellan en effektiv brottsbekämpning och skyddet av enskildas integritet. *Hovrätten för Västra Sverige* och *JO* anser att det i viss mån finns en risk för att principen om förbud mot självinkriminering åsidosätts. *Myndigheten för samhällsskydd och beredskap (MSB), Hovrätten för Västra Sverige, Post- och telestyrelsen* och *Sveriges advokatsamfund* har synpunkter på bestämmelsernas tillämpning i förhållande till proportionalitetsprincipen.

Bahnhof AB, Post- och telestyrelsen och *Internetstiftelsen* uttrycker oro över att den föreslagna skyldigheten att bevara lagrade uppgifter kan uppfattas som en utökad skyldighet att inskaffa eller lagra uppgifter i förväg och över att ett föreläggande om bevarande kan vara generellt, t.ex. avse samtliga e-postmeddelanden som förmedlats via en viss server. *IT & Telekomföretagen, Rättighetsalliansen, Internetstiftelsen, Svenska journalistförbundet* och *Sveriges advokatsamfund* påpekar att bestämmelserna kan komma i konflikt med bestämmelser om sekretess och tystnadsplikt i annan lagstiftning och att de kan medföra lojalitetskonflikter för den som har förelagts. *Ekobrottsmyndigheten, Hovrätten för Västra Sverige* och *Åklagarmyndigheten* ifrågasätter om straffbestämmelsen i 17 kap. 13 § brottsbalken är en tillräcklig sanktion för att bestämmelsen ska få avsedd effekt. *Ekobrottsmyndigheten, Polismyndigheten, Rättighetsalliansen, Säkerhetspolisen* och *Åklagarmyndigheten* efterfrågar en utökad möjlighet till förlängning av tiden för ett bevarande. *Hovrätten över Skåne och Blekinge* ifrågasätter utrymmet för muntliga förelägganden på grund av risken för oklarheter och har, liksom *IT & Telekomföretagen*, synpunkter på mot vem ett föreläggande ska riktas. *Domstolsverket, Helsingborgs tingsrätt, Hovrätten för Skåne och Blekinge, Hovrätten för Västra Sverige, JO, Juliagruppen, Post- och telestyrelsen, Rättighetsalliansen* och

Säkerhetspolisen har synpunkter på bestämmelsernas utformning och avgränsning. *MSB* anser att en rad praktiska aspekter av förslaget behöver tydliggöras.

Skälen för regeringens förslag

En möjlighet till frysning av uppgifter införs

Brottsutredande myndigheter ska enligt konventionen ha möjlighet att skyndsamt säkra särskilt angivna datorbehandlingsbara uppgifter som redan finns lagrade (se artikel 16). Artikeln syftar till att ge brottsutredande myndigheter möjlighet att under en begränsad tidsperiod säkra lagrade datorbehandlingsbara uppgifter i avvaktan på ett eventuellt beslut om andra tvångsåtgärder, en form av s.k. frysning. Ett säkrande innebär att uppgifterna ska bevaras på ett betryggande sätt.

De uppgifter som avses kan vara av vilket slag som helst, t.ex. en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat. Att uppgiften ska vara lagrad betyder att den ska finnas bevarad elektroniskt. Både sådana uppgifter som finns lagrade på grund av regler om datalagring och sådana som lagrats av annan anledning omfattas alltså. Förslaget innebär ingen utökad skyldighet att lagra elektronisk information. Uppgiften måste finnas lagrad när föreläggandet meddelas. Det går inte att förelägga någon att framöver lagra eller spara uppgifter.

Föreläggandet ska avse en viss elektronisk uppgift. Det innebär att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan alltså inte vara generellt och t.ex. utan närmare specificering endast ange att alla uppgifter som mottagits under en tid ska bevaras. Ett säkrande ska kunna göras både hos fysiska och juridiska personer, inklusive tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster.

Det finns i dag ingen motsvarighet till en sådan åtgärd i svensk rätt. För att uppfylla kraven i artikel 16 behöver därför en möjlighet till skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter införas.

Både *Polismyndigheten, Säkerhetspolisen* och *Ekobrottsmyndigheten* anför att möjligheten att kunna utfärda ett föreläggande om bevarande är ett efterlängtat verktyg inom brottsbekämpningen. Som *Rättighetsalliansen* påpekar kan möjligheten till bevarande i förlängningen också innebära en förstärkning av integriteten för de som blir utsatta för brott och kränkningar på internet. Flera remissinstanser, bl.a. *JO*, *Datainspektionen* och *Post- och telestyrelsen,* invänder att ett bevarande innebär ett intrång i den enskildes integritet och efterfrågar en tydligare behovsanalys. Som Datainspektionen påpekar har regeringen i tidigare sammanhang bedömt att redan själva lagringen av uppgifter utgör ett integritetsintrång, eftersom åtgärden bidrar till enskildas upplevelse av att få sin privata sfär och frihet inskränkt (se propositionerna Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG, prop. 2010/11:46 s. 19 och Datalagring vid brottsbekämpning – anpassningar till EU-rätten, prop. 2018/19:86 s. 34).

Även ett bevarande av redan lagrade uppgifter kan bidra till enskildas upplevelse av att få sin privata sfär och frihet inskränkt (se t.ex. EU-

domstolens dom den 6 oktober 2020 i mål C 511/18, C 512/18 och C 520/18). Införandet av en möjlighet till föreläggande om bevarande kräver därför att åtgärden är välmotiverad. Det integritetsintrång ett föreläggande innebär är emellertid förhållandevis begränsat. Ett föreläggande enligt den föreslagna bestämmelsen ska vara avgränsat till en viss uppgift, kan bara avse uppgifter som redan finns lagrade och medför endast en skyldighet att bevara en uppgift under en viss tid, inte att lämna ut den. Ett föreläggande om bevarande kommer alltså inte, som bl.a. *Sveriges advokatsamfund* befarar, medföra att enskilda måste agera angivare eller tvingas åsidosätta sekretess eller tystnadsplikt i andra lagar. Ett föreläggande om bevarande kommer inte heller, som bl.a. *Bahnhof AB*, *Post- och telestyrelsen* och *Internetstiftelsen* befarar, att innebära en utökad skyldighet att inskaffa eller lagra uppgifter i förväg och inte heller en möjlighet till generella förelägganden om bevarande, t.ex. av samtliga e-postmeddelanden som förmedlats via en viss server.

De brottsutredande myndigheterna framhåller att det finns ett stort behov av en möjlighet till föreläggande om bevarande. Utredningen av vissa it-relaterade brott, t.ex. barnpornografibrott, förutsätter att de brottsbekämpande myndigheterna får tillgång till uppgifter om elektronisk kommunikation. Det medför ett ökat behov av att snabbt kunna säkra och bevara vissa lagrade elektroniska uppgifter. Tillgången till ett verktyg för frysning av uppgifter innebär också ökade möjligheter till ett effektivt internationellt samarbete vid bekämpningen av it-relaterade brott. I vissa fall ger det också de brottsbekämpande myndigheterna ett mindre ingripande alternativ till åtgärder som husrannsakan, edition och beslag, liksom de hemliga tvångsmedlen.

Regeringen anser sammantaget att utredningens förslag om föreläggande om bevarande är välmotiverat och, i likhet med bl.a. *JK*, väl avvägt med hänsyn till behovet av åtgärden, åtgärdens effektivitet och de integritetsaspekter som gör sig gällande. Det bör därför införas en möjlighet att förelägga någon att under en viss tid bevara lagrade elektroniska uppgifter. Åtgärden är att betrakta som ett straffprocessuellt tvångsmedel och bör placeras i 27 kap. rättegångsbalken.

Vem ska ett föreläggande kunna riktas mot?

Ett föreläggande ska kunna riktas mot den som innehar uppgifterna (se artikel 16). Det innebär att uppgifterna antingen ska finnas lagrade hos personen eller på annat sätt vara under personens kontroll och åtkomst. I det senare fallet kan uppgifterna finnas lagrade på en server någon annanstans än där personen befinner sig. Lagrade uppgifter kan också innehas av flera olika personer samtidigt, t.ex. om en person har sin e-post lagrad på en server hos en annan person. Ett föreläggande bör då kunna riktas mot såväl den som uppgifterna finns lagrade hos som den som på distans har kontroll över och åtkomst till uppgifterna.

Hovrätten över Skåne och Blekinge efterfrågar ytterligare förtydliganden av vilka ett föreläggande om bevarande ska kunna riktas mot. Uttrycket ”den som” innebär att föreläggandet ska kunna rikta sig mot både fysiska och juridiska personer, inklusive tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster. Det bör ytterst vara den som beslutar om föreläggandet som också beslutar mot vem det ska riktas

i varje enskilt ärende. Att, som *IT&Telekomföretagen* föreslår, låta systemägaren ha inflytande över vem som ska föreläggas kan försvåra brottsutredningen. Det finns emellertid inte några hinder mot att den som beslutar om ett föreläggande vid behov rådfrågar systemägaren.

Konventionen förutsätter att ett säkrande ska kunna ske hos både enskilda och juridiska personer (se artikel 16). *Sveriges advokatsamfund* anser att de bevis som kan säkras genom förelägganden mot enskilda personer kommer att vara av liten betydelse. Som framgår i det följande innebär proportionalitetsprincipen att ett föreläggande om bevarande inte får utfärdas om det finns skäl att tro att uppgifterna inte kommer att kunna begäras utlämnade eller på annat sätt tas om hand i ett senare skede. Vad advokatsamfundet framfört anses inte utgöra tillräckliga skäl att begränsa regeln till att endast omfatta juridiska personer.

När ska ett föreläggande beslutas?

Tidpunkten för när i en brottsutredning ett föreläggande om bevarande ska kunna beslutas framgår inte av konventionen. Regeringen delar utredningens bedömning att ett föreläggande ska kunna beslutas när någon innehar en viss lagrad uppgift i elektronisk form som skäligen kan antas ha betydelse för utredningen om ett brott. Ett säkrande av elektroniska uppgifter måste kunna göras i ett tidigt skede av en brottsutredning, på samma sätt som gäller för beslag och kvarhållande av försändelse.

JO och *Hovrätten för Västra Sverige* uppmärksammar risken för att bestämmelsens utformning kan strida mot förbudet mot självinkriminering om den person som förelagts att bevara en uppgift i ett senare skede blir misstänkt för brottet. Redan i dag förutsätter reglerna om förundersökningar i brottmål att den som blir skäligen misstänkt för ett brott kan vara skyldig att medverka i utredningen i ett tidigare skede. Regeringen har i samband med genomförandet av Europaparlamentets och rådets direktiv (EU) 2016/343 om förstärkning av vissa aspekter av oskuldspresumtionen och av rätten att närvara vid rättegången i straffrättsliga förfaranden bedömt att det är en nödvändig ordning som inte i sig står i strid med förbudet mot självinkriminering (se propositionen Genomförande av oskuldspresumtionsdirektivet, prop. 2017/18:58 s. 10). Förbudet mot självinkriminering bör mot denna bakgrund kunna upprätthållas med de föreslagna bestämmelserna.

Om ett föreläggande om bevarande ska vara ett effektivt verktyg för de brottsutredande myndigheterna bör något krav inte ställas på att förundersökningen har kommit så långt att någon är skäligen misstänkt för brottet. Om det finns en skäligen misstänkt person ska ett föreläggande emellertid inte kunna riktas mot honom eller henne. Inte heller bör ett föreläggande kunna riktas mot den misstänktes närstående. Som utredningen föreslår bör detta framgå av författningstexten.

Ska åtgärden vara begränsad till vissa situationer?

Enligt utredningens förslag ska möjligheten att utfärda ett föreläggande om bevarande inte vara begränsad till vissa brottstyper eller till brott av viss svårhetsgrad.

En åtgärd om säkrande ska kunna tillämpas i förhållande till de brott som omfattas av konventionen och andra brott som begåtts med hjälp av

ett datorsystem samt generellt på insamling av bevis i elektronisk form om ett brott (se artikel 14.2). Även om konventionen förutsätter en generell möjlighet till säkringsåtgärder i dessa fall finns ett visst utrymme att i den nationella lagstiftningen närmare reglera vilka förutsättningar som ska vara uppfyllda för att åtgärden ska få vidtas.

Vid beslut om och användning av tvångsmedel gäller proportionalitetsprincipen (se t.ex. 27 kap. 1 § tredje stycket och 28 kap. 3 a § rättegångsbalken). Den innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet alltid ska stå i rimlig proportion till vad som står att vinna med den (se t.ex. propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation, prop. 2011/12:55 s. 72). Proportionalitetsprincipen kommer att vara tillämplig även i fråga om den nu aktuella åtgärden. Det innebär att ett föreläggande om bevarande inte kommer att kunna meddelas om det inte finns ett tillräckligt starkt behov av åtgärden med beaktande av motstående intressen.

Det är inte alltid möjligt att i ett tidigt skede av en utredning avgöra brottets rubricering eller svårhetsgrad. Det kan även vara svårt att så tidigt i utredningen förutse vilken betydelse ett bevis kommer att få. Regeringen delar därför utredningens bedömning att det inte är lämpligt att möjligheten att meddela ett föreläggande kopplas till en viss typ av brott eller till brott av en viss svårhetsgrad, som *Sveriges advokatsamfund* och *Post- och telestyrelsen* föreslår. Regeringen bedömer vidare att möjligheten att meddela ett föreläggande inte heller ska vara begränsad på annat sätt än att det skäligen kan antas att en viss uppgift kan ha betydelse för utredningen om ett brott. Förslaget är i denna del utformat i huvudsak på samma sätt som reglerna om beslag, vilket är en åtgärd som många gånger kan anses vara mer ingripande från ett integritetsperspektiv (se 27 kap. 1 § första stycket rättegångsbalken).

Flera av de farhågor om brytande av källskydd och brott mot tystnadsplikt som bl.a. *Sveriges advokatsamfund* och *Svenska Journalistförbundet* ger uttryck för gör sig huvudsakligen gällande först när uppgifter lämnas ut eller tas i beslag. Lagring eller bevarande av uppgifter kan inte i sig medföra ett åsidosättande av källskydd, advokatsekretess eller annan tystnadsplikt. Som anges ovan kan emellertid ett föreläggande om bevarande uppfattas som en förberedande åtgärd till något sådant. Det ska därför särskilt framhållas att proportionalitetsprincipen också innebär att de brottsbekämpande myndigheterna inte bör meddela ett föreläggande om bevarande om de kan se att det mot bakgrund av brottets allvar eller av andra skäl inte finns någon möjlighet att senare få ut uppgifterna. T.ex. omöjliggör bestämmelsen om beslagsförbud ett senare beslag av uppgifter relaterade till förtrolig korrespondens mellan en advokat och hans eller hennes klient eller uppgifter som omfattas av källskyddet enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen (27 kap. 2 § rättegångsbalken).

Den föreslagna regleringen är alltså enligt regeringens bedömning tillräckligt begränsad för att inte inverka på bestämmelser om sekretess och källskydd som finns i annan lagstiftning. Eftersom en proportionalitetsbedömning måste göras i varje enskilt fall finns det inte något behov av att, som *Hovrätten för Västra Sverige* föreslår, införa uttryckliga bestämmelser om när ett föreläggande om bevarande inte får beslutas.

Föreläggandets innehåll och form

Den som innehar en viss lagrad elektronisk uppgift bör kunna åläggas att se till att uppgiften bevaras på ett sådant sätt att den inte kan förstöras, förändras eller på annat sätt göras oåtkomlig. Föreläggandet bör som huvudregel ges skriftligen. Eftersom föreläggandet avser en viss uppgift bör det anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Regeringen delar därmed inte *Bahnhof AB:s* oro för storskaliga körningar.

MSB undrar om det kommer att ställas några krav på att informationshanteringen vid ett bevarande sker på ett visst sätt. Regeringen instämmer i utredningens bedömning att ett bevarande bör kunna ske på olika sätt. Ett alternativ är att den som föreläggandet riktar sig mot kopierar uppgiften. Ett annat alternativ är att uppgiften lämnas orubbad på sin ursprungliga plats, samtidigt som åtgärder vidtas så att den inte kan raderas eller ändras på något sätt. Olika mottagare av ett föreläggande kan förväntas ha olika resurser och förutsättningar för att efterleva det. Vid behov får den som har beslutat om föreläggandet ge anvisningar om hur uppgiften ska bevaras i det enskilda fallet. Sådana anvisningar kan ges i samråd med den som föreläggandet riktar sig mot.

Hovrätten över Skåne och Blekinge anser att ett föreläggande alltid ska ges skriftligen. Regeringen delar hovrättens uppfattning att det är viktigt att föreläggandets innebörd framgår tydligt. Föreläggandet bör som huvudregel därför ges i skriftlig form. Situationer kan emellertid uppstå då det finns ett behov av att meddela ett föreläggande muntligt, exempelvis om ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande. Det bör därför inte införas något krav på att föreläggandet ska vara skriftligt. Däremot behöver föreläggandet dokumenteras skriftligt och tillställas den som har förelagts åtgärden så snart det är möjligt.

Tiden för bevarande

De uppgifter som omfattas av föreläggandet ska bevaras så länge det behövs men 90 dagar som längst i ett första skede. Det får också finnas en möjlighet att förlänga den tiden med 90 dagar (se artikel 16.2).

Tiden för bevarande bör aldrig vara längre än nödvändigt. I de allra flesta fall bör 90 dagar vara en fullt tillräcklig tid för att de brottsutredande myndigheterna ska hinna avgöra om de ska vidta åtgärder för att få tillgång till uppgifterna. I mer komplicerade fall, t.ex. när ett ärende har internationell anknytning, kan det dock som flera remissinstanser framfört krävas en längre tid för bevarande än 90 dagar. Regeringen anser därför, i likhet med utredningen, att tiden för bevarande ska kunna bestämmas till högst 90 dagar i ett första skede och att det även bör finnas en möjlighet att förlänga den tiden om det finns särskilda skäl för det.

Enligt utredningens förslag ska den ursprungliga tiden för bevarande få förlängas med högst 30 dagar. Den valda förlängningsfristen, som alltså är kortare än de 90 dagar som konventionen medger, motiveras inte särskilt. Som exempel på fall där en förlängning kan vara motiverad tar utredningen upp brottsutredningar med internationell anknytning. Utredningen betonar också att ett bevarande aldrig bör vara längre än nödvändigt i det enskilda fallet.

Regeringen anser i likhet med utredningen att det är av stor vikt att tiden för bevarande i det enskilda fallet inte ska vara längre än nödvändigt med hänsyn till de integritetsaspekter som gör sig gällande. Utredningens förslag att ett föreläggande om bevarande ska kunna förlängas med upp till endast 30 dagar möter emellertid kritik. Remissinstanser som *Ekobrottsmyndigheten, Polismyndigheten, Rättighetsalliansen, Säkerhetspolisen* och *Åklagarmyndigheten* framför att en längsta tid för förlängning om 30 dagar är för kort, särskilt i ärenden med internationell anknytning som över lag präglas av en viss tröghet.

Utredningar om it-relaterad brottslighet har inte sällan internationella inslag. Det kan vara fråga om en nationell förundersökning där de svenska brottsbekämpande myndigheterna måste invänta information från eller åtgärder i utlandet för att kunna besluta om sådana uppgifter som bevaras på grund av ett föreläggande behövs. Det kan också röra sig om rent internationella fall där rättslig hjälp med ett föreläggande om bevarande begärts i Sverige eller där Sverige verkställer en europeisk utredningsorder för samma åtgärd. I samtliga fall finns det behov av att kunna bevara uppgifterna tills det andra landet har hunnit vidta nödvändiga åtgärder. Det finns därför stora fördelar med en enhetlig frist för det nationella regelverket och för de regler som styr det internationella samarbetet. Regelverken blir också lättare att tillämpa och mer förutsebara om samma frist gäller. Enhetlighet minskar också risken för felaktig tillämpning, vilket är centralt ur ett rättssäkerhetsperspektiv.

Utredningen lämnade sitt betänkande innan lagen (2017:1000) om en europeisk utredningsorder infördes. Utredningens förslag om en längsta tid för förlängning med 30 dagar har därför inte kunnat utformas med beaktande av förutsättningarna i den lagen eller det bakomliggande EU-direktivet (se artikel 12 i direktivet). Direktivets tidsfrister innebär bl.a. att den verkställande staten har upp till 120 dagar på sig att erkänna och verkställa en mottagen europeisk utredningsorder. En order för ett föreläggande om bevarande behöver kunna bestå under den tid det tar för en efterföljande order om att uppgifterna ska röjas att erkännas och verkställas.

Regeringen menar att den kritik som remissinstanserna lämnar mot förslaget måste tas på allvar. De 30 dagar som utredningen har föreslagit synes inte i alla situationer vara en tillräckligt lång frist för att uppnå det resultat som konventionens möjlighet till förlängning syftar till. Detta blir särskilt tydligt i brottsutredningar med internationella inslag, något som förekommer i många utredningar om it-relaterad brottslighet. Mot den bakgrunden bedömer regeringen, till skillnad från utredningen, att det inte finns skäl att föreskriva en kortare förlängningsmöjlighet än den konventionen medger. Det bör alltså vara möjligt att förlänga den ursprungliga tiden för bevarande med högst 90 dagar om det finns särskilda skäl för det.

Genom kravet på att det i det enskilda fallet ska finnas särskilda skäl för en förlängning garanteras ändå en rimlig avvägning mellan behovet av en effektiv reglering och det integritetsintrång ett bevarande kan innebära för den som drabbas av åtgärden. Kravet på särskilda skäl innebär att den fulla förlängningsmöjligheten bara får utnyttjas i undantagsfall och att fristen aldrig får bestämmas till längre än vad som är nödvändigt. Tiden kan förlängas vid ett eller flera tillfällen så länge den maximala fristen om 90 dagar plus 90 dagars förlängning inte överskrids.

I avsnitt 6.1.3 görs ytterligare överväganden beträffande lagen om en europeisk utredningsorder.

Tystnadsplikt

Den som föreläggs att bevara en viss lagrad uppgift ska kunna åläggas att hemlighålla att en sådan åtgärd har vidtagits (se artikel 16.3). Det finns inga bestämmelser om tystnadsplikt som träffar den situationen i svensk rätt. Tystnadsplikt på grund av förundersökningssekretess kan beslutas under andra skeden av ett förfarande (se t.ex. 23 kap. 10 § sista stycket rättegångsbalken). Det finns också en möjlighet att vid förordnanden om att en försändelse ska hållas kvar besluta att den som mottagit försändelsen för befordran inte får lämna meddelande om åtgärden utan tillstånd (se 27 kap. 9 § rättegångsbalken). Regeringen delar utredningens bedömning att även ett föreläggande om att bevara en viss lagrad uppgift ska kunna innehålla en underrättelse om att den som förelagts inte får uppenbara att åtgärden vidtagits. Detta bör framgå uttryckligen av bestämmelsen.

Regeringens förslag innebär inte att den föreslagna tystnadsplikten har företräde framför den grundlagsskyddade rätten att meddela och offentliggöra uppgifter.

Juliagruppen anser att tystnadsplikten bör tidsbestämmas. Tystnadsplikten är en del av föreläggandet och gäller som huvudregel till dess att föreläggandet inte längre gäller, rätten upphävt föreläggandet eller åklagaren eller förundersökningsledaren meddelat något annat. Regeringen bedömer därför att den föreslagna bestämmelsen om tystnadsplikt är tillräckligt avgränsad.

Beslutsordning

En fördragsslutande part ska vidta nödvändiga åtgärder för att ett säkrande av lagrade datorbehandlingsbara uppgifter ska kunna ske skyndsamt (se artikel 16). Det finns ett behov av att snabbt kunna säkra viss lagrad information i ett tidigt skede för att kunna bedriva effektiva brottsutredningar. Ett föreläggande om att bevara en viss lagrad uppgift bör därför kunna meddelas av en åklagare eller en annan förundersökningsledare. I de fall Tullverket med stöd av 19 § lagen (2000:1225) om straff för smuggling inlett en förundersökning kommer även Tullverket ha möjlighet att besluta om ett föreläggande. Detsamma gäller Kustbevakningen när en förundersökning inletts med stöd av 3 kap. 3 § kustbevakningslagen (2019:32).

Eftersom det är fråga om en tvångsåtgärd bör den som förelagts, i likhet med vad som gäller vid beslag, kunna begära rättens prövning av föreläggandet. Rättens prövning bör också kunna avse tiden för bevarande.

Rättegångsbalkens regler om rättens prövning av ett beslag bör tillämpas, vilket innebär att 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 (se 27 kap. 6 § rättegångsbalken). *Helsingborgs tingsrätt* anser att ett allmänt skyndsamhetskrav är tillräckligt och att kravet på att rätten ska hålla förhandling inom fyra dagar inte behövs. Regeringen bedömer emellertid att en skyndsam prövning är nödvändig för att kunna ta tillvara rätten för den som förelagts. Utan tidsfrist för prövningen finns det risk för att den tid för bevarande som ställts

upp i föreläggandet hinner gå till ända innan rätten har hunnit pröva frågan. Reglerna i 27 kap. 6 § rättegångsbalken bör därför vara tillämpliga.

Det behövs inga ytterligare sanktionsmöjligheter

Konventionen kräver inte att det införs några sanktioner mot den som inte följer ett föreläggande om bevarande, även om artikel 16 naturligtvis förutsätter ett effektivt genomförande av bestämmelsen. Det huvudsakliga syftet med ett föreläggande är att förhindra att en uppgift försvinner på grund av ett systems funktion, gällande rutiner eller annan lagstiftning. Brottsbalkens straffbestämmelse om överträdelse av myndighets bud bör kunna tillämpas i fall då någon aktivt raderar en uppgift i strid med ett föreläggande om att bevara den (se 17 kap. 13 §). Även den som medverkar till ett sådant brott kan dömas till ansvar (se 23 kap. 4 §). När det gäller beslut om tystnadsplikt bör ett brott mot yppandeförbudet kunna föranleda böter (se 9 kap. 6 § rättegångsbalken).

JO, Hovrätten för Västra Sverige, Åklagarmyndigheten, Ekobrottsmyndigheten och *Rättighetsalliansen* efterfrågar bättre sanktionsmöjligheter för att göra regleringen effektiv. Majoriteten av de personer som ett föreläggande kommer att riktas mot kan förväntas sakna anledning att motsätta sig det. I de fall där den förelagde aktivt vidtar åtgärder i strid med ett föreläggande bedöms befintliga sanktionsmöjligheter vara tillräckliga för att garantera reglernas efterlevnad.

Behov av ändringar i lagen om elektronisk kommunikation

Elektroniska uppgifter behöver kunna säkras hos tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Det bör återigen framhållas att ett föreläggande om bevarande ska avse en viss lagrad uppgift, vilket innebär dels att uppgiften redan måste finnas lagrad hos den som föreläggandet riktar sig mot, dels att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras. Föreläggandet kan varken innebära att uppgifter som inte är lagrade ska inhämtas och bevaras eller gälla hela servrar hos företag. Med lagrad uppgift avses alla uppgifter som finns lagrade av någon anledning, dvs. både sådana uppgifter som finns lagrade på grund av regler om datalagring och sådana som lagrats av annan anledning. Det kan t.ex. vara uppgifter som hos tillhandahållaren behandlas för fakturahantering eller liknande.

Ett föreläggande kommer alltså även att kunna riktas mot den tillhandahållare som bedriver verksamhet som är anmälningspliktig enligt lagen om elektronisk kommunikation och avse sådana uppgifter som lagrats för brottsbekämpande ändamål enligt den lagen. Lagens särskilda bestämmelser om kvalitet och säkerhet när det gäller uppgifter som lagrats för brottsbekämpande syften, om rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut och om anpassning för utlämnande av uppgifter ska enligt utredningens förslag tillämpas även när uppgifter bevaras hos tillhandahållaren på grund av att tillhandahållaren ålagts ett föreläggande om bevarande (se 6 kap. 3 a, 16 e och 16 f §§).

Säkerhetspolisen och *Post- och telestyrelsen* ifrågasätter den avgränsning som utredningen har gjort och saknar resonemang om ersättning för kostnader samt om kvalitet och säkerhet när ett föreläggande om bevarande avser uppgifter hos aktörer som inte är anmälningspliktiga eller inte

omfattas av lagen om elektronisk kommunikation. Även om ett föreläggande om bevarande kan riktas mot vem som helst som har en elektronisk uppgift lagrad bedöms tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bli föremål för ett föreläggande om bevarande i betydligt högre utsträckning än andra tjänsteleverantörer. Det är en följd av den lagringsskyldighet som följer av lagen om elektronisk kommunikation. Samma regler om skyddskrav och rätt till ersättning i lagen om elektronisk kommunikation bör gälla oberoende av om en viss uppgift lagras för brottsbekämpande ändamål eller bevaras enligt ett föreläggande om bevarande. Det ska för tydlighets skull framhållas att tiden för bevarande enligt ett föreläggande inte påverkar den tid en uppgift enligt 6 kap. 16 d § ska hållas lagrad.

Regeringen anser mot denna bakgrund att det finns anledning att i viss mån särbehandla de aktörer som omfattas av lagringsskyldigheten i lagen om elektronisk kommunikation även vid bevarande av uppgifter i anledning av ett föreläggande om bevarande. Reglerna om kvalitet och säkerhet, om rätt till ersättning för kostnader och om anpassning för utlämnande bör alltså tillämpas när uppgifter bevaras hos en tjänsteleverantör på grund av ett föreläggande. En bestämmelse om det bör tas in i den lagen. Det kan nämnas att frågan om ersättning är föremål för överväganden i promemorian Registrering av kontantkort, m.m. (Ds 2020:12). Promemorian bereds för närvarande i Regeringskansliet.

Regeringen delar utredningens bedömning att bestämmelserna om att lagrade uppgifter i vissa fall inte ska utplånas ska omfatta uppgifter som begärts bevarade och att tystnadsplikt även ska gälla för uppgifter som hänför sig till ett föreläggande om bevarande (se 6 kap. 8 och 16 d §§ samt 20 § första stycket). Jämfört med utredningens förslag föreslår regeringen att undantag från reglerna om utplåning regleras i 6 kap. 8 § istället för i 6 kap. 5 §. Att tystnadsplikten också bör gälla när uppgifter om andra tillhandahållare begärs ut framgår av avsnitt 6.2.

Tystnadsplikten i lagen om elektronisk kommunikation omfattar den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till en uppgift som hänför sig till ett föreläggande om bevarande. Den kommer alltså delvis att överlappa den tystnadsplikt som föreslås i rättegångsbalken men avser en vidare krets av personer. Regeringens förslag innebär inte att den föreslagna tystnadsplikten har företräde framför den grundlagsskyddade rätten att meddela och offentliggöra uppgifter.

6.1.2 Det ska vara möjligt att lämna internationell rättslig hjälp med ett föreläggande om bevarande

Regeringens förslag: Sverige ska kunna begära och lämna rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken.

En ansökan om sådan rättslig hjälp ska handläggas av en åklagare. Rättslig hjälp med ett föreläggande ska få lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag.

Sverige ska avge en förklaring om att Sverige ska förbehålla sig rätten att avslå en framställning om rättslig hjälp med ett föreläggande om bevarande, om det finns skäl att tro att uppgifterna inte kommer att kunna röjas i ett senare skede på grund av ett krav på dubbel straffbarhet.

Regeringens bedömning: Det finns tillräckliga rättssäkerhetsgarantier för den som har förelagts att bevara en viss uppgift i befintlig reglering även utan ett krav på dubbel straffbarhet.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Polismyndigheten* och *Säkerhetspolisen* anser att möjligheten till rättslig hjälp med ett föreläggande om bevarande innebär en efterlängtad harmonisering i det internationella samarbetet.

Skälen för regeringens förslag och bedömning

Sverige ska kunna lämna internationell rättslig hjälp med ett föreläggande om bevarande

Ömsesidig rättslig hjälp ska kunna lämnas med ett sådant skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter som avses i artikel 16 i konventionen (se artikel 29). Som huvudregel får något krav inte ställas på att rättslig hjälp får lämnas endast om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), i vart fall inte för sådana brott som är upptagna i artiklarna 2–11. Konventionen reglerar också de närmare förutsättningarna för en ansökan om rättslig hjälp, bl.a. vilka uppgifter den ska innehålla, under hur lång tid ett föreläggande ska gälla i dessa situationer, under vilka förutsättningar ansökan får avslås och att den ska prövas skyndsamt.

För att en svensk myndighet ska kunna lämna rättslig hjälp med en tvångsåtgärd krävs att åtgärden finns tillgänglig i nationell rätt och omfattas av regleringen i lagen (2000:562) om internationell rättslig hjälp i brottmål. Utgångspunkten är att alla åtgärder som är möjliga att vidta i en svensk förundersökning även 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 (se propositionen Internationell rättslig hjälp i brottmål, prop. 1999/2000:61 s. 79).

Nu föreslås en möjlighet till föreläggande om bevarande nationellt. För att skapa en möjlighet att också lämna internationell rättslig hjälp med åtgärden bör föreläggande om bevarande föras in i den paragraf i lagen om internationell rättslig hjälp i brottmål som anger vilka åtgärder som omfattas av rättslig hjälp enligt lagen (se 1 kap. 2 §).

Den ordning som ska gälla för rättslig hjälp med ett föreläggande bör i så stor utsträckning som konventionen tillåter följa befintlig systematik i lagen. Hjälp bör därför som utgångspunkt lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång (se 2 kap. 1 §). Det innebär bl.a. att ett föreläggande om bevarande som huvudregel ska ges skriftligt. Vidare får det inte riktas mot den som skäligen kan misstänkas för brottet eller mot någon till honom eller henne sådan närstående person som avses i 36 kap. 3 §

rättegångsbalken (se förslaget till 27 kap. 16 och 16 a §§ rättegångsbalken). Det innebär också att det alltid måste göras en proportionalitetsbedömning innan åtgärden beslutas (se 27 kap. 1 § rättegångsbalken).

Konventionen ställer krav på att en ansökan ska innehålla de uppgifter som behövs för att åtgärden ska kunna genomföras, bl.a. information om vilka lagrade uppgifter som ska säkras och var och hos vem uppgifterna finns. Att en ansökan om rättslig hjälp ska innehålla sådan information framgår redan av lagen och några särskilda bestämmelser om det behövs inte (se 2 kap. 4 §). Krav ställs också på att en ansökan ska prövas skyndsamt. Utgångspunkten bör alltså vara att ansökan, liksom vid nationella förhållanden, prövas av en åklagare. Det behövs därför också en bestämmelse om detta.

Det bör, som utredningen föreslagit, även i internationella situationer finnas en möjlighet att överklaga för den som drabbas av en åtgärd (se förslaget till 27 kap. 16 a § rättegångsbalken). För beslut enligt lagen om internationell rättslig hjälp i brottmål gäller att samma regler tillämpas som för ett nationellt förfarande (se 2 kap. 1 §). Några särskilda regler om överklagande behövs därför inte.

Eftersom rättslig hjälp ska lämnas under samma förutsättningar som en motsvarande åtgärd under en svensk förundersökning får föreläggandet inte heller gälla längre än den tid som anges i förslaget till 27 kap. 16 § andra och tredje stycket rättegångsbalken. Det innebär att tiden inte får bestämmas till längre än nödvändigt och högst 90 dagar i ett första skede, med en möjlighet till förlängning med ytterligare högst 90 dagar om det finns särskilda skäl. Skälen för en förlängningsmöjlighet om 90 dagar istället för den frist om 30 dagar som utredningen föreslagit redovisas i avsnitt 6.1.1.

Inget krav på dubbel straffbarhet

De konventionsslutande parterna får inte ställa upp krav på dubbel straffbarhet för att lämna rättslig hjälp med ett föreläggande om bevarande för de brott som räknas upp i artikel 2–11 i konventionen och 3–7 i tilläggsprotokollet (se artikel 29.3 och 4 i konventionen och artikel 8.2 i tilläggsprotokollet). Rättslig hjälp med ett föreläggande om bevarande kan däremot vägras om det vid beslutstidpunkten finns skäl att tro att de uppgifter som begärs bevarade inte kommer att kunna lämnas ut i ett senare skede på grund av ett krav på dubbel straffbarhet, under förutsättning att ett land har förbehållit sig den rätten (se artikel 29.4).

Enligt regeringen finns det, även utan en reglering som förutsätter dubbel straffbarhet, i den svenska befintliga ordningen tillräckliga rättssäkerhetsgarantier för den som förelagts i sådana situationer (se 2 kap. 14 § lagen om internationell rättslig hjälp i brottmål). Något krav på dubbel straffbarhet för rättslig hjälp med ett föreläggande om bevarande bedöms därför inte vara nödvändigt (se 2 kap. 2 §).

Om det vid beslutstidpunkten finns skäl att tro att de uppgifter som begärs bevarade inte kommer att kunna lämnas ut i ett senare skede på grund av ett krav på dubbel straffbarhet, bör dock rättslig hjälp kunna vägras med stöd av 2 kap 14 §. Som utredningen föreslagit bör Sverige alltså utnyttja möjligheten till förbehåll i artikel 29.4 i konventionen, även om möjligheten att vägra rättslig hjälp bör användas restriktivt.

Grundlagsskyddade gärningar

Gärningar som omfattas av tryckfrihetsförordningen och yttrandefrihetsgrundlagen kan endast lagföras i den ordning och omfattning som föreskrivs där. Om en begäran om rättslig hjälp med ett föreläggande om bevarande enligt lagen om internationell rättslig hjälp i brottmål skulle komma i konflikt med bestämmelserna i dessa svenska grundlagar, bör rättslig hjälp vägras. Ett uttryckligt stöd för en sådan ordning finns i artikel 29.5 b i Budapestkonventionen och 2 kap. 14 § i lagen om internationell rättslig hjälp i brottmål. Någon särskild vägransgrund med hänvisning till grundlagarna behöver därför inte införas (jfr propositionen Nya regler om bevisinhämtning inom EU, prop. 2016/17:218 s. 138 och propositionen Internationell rättslig hjälp i brottmål, prop. 1999/2000:61 s. 73).

6.1.3 En europeisk utredningsorder ska kunna avse ett föreläggande om bevarande

Regeringens förslag: En utredningsorder ska kunna avse ett föreläggande om att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken.

En utredningsorder för ett föreläggande om bevarande ska utfärdas av en åklagare. När utredningsordern har verkställts i den andra medlemsstaten ska den som förelagts att bevara en viss lagrad uppgift kunna begära rättens prövning av åtgärden. Tiden för bevarande ska räknas från verkställighetstidpunkten i den andra medlemsstaten. Den tid för bevarande om högst 90 dagar som anges i förslaget till 27 kap. 16 § andra stycket rättegångsbalken ska få förlängas med högst 90 dagar om det finns särskilda skäl.

En åklagare ska pröva om en utredningsorder för ett föreläggande om bevarande ska erkännas och verkställas i Sverige. När utredningsordern har verkställts i Sverige ska den som har förelagts att bevara en viss lagrad uppgift kunna begära rättens prövning av verkställbarhetsförklaringen.

En utredningsorder ska kunna erkännas och verkställas även om den gärning som avses inte motsvarar ett brott enligt svensk lag. Om åtgärden riktar sig mot den som skäligen kan misstänkas för brottet eller mot någon till honom eller henne sådan närstående person som avses i 36 kap. 3 § rättegångsbalken ska erkännande av utredningsordern vägras.

Den kompletterande promemorians förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Sveriges advokatsamfund* avstyrker förslagen eftersom det bakomliggande förslaget om en möjlighet till föreläggande om bevarande avstyrks. Om det införs en möjlighet till föreläggande om bevarande har samfundet emellertid inget att invända mot promemorians förslag. *JO* anser att en möjlighet till sammanlagd tid för bevarande om 90 plus 90 dagar framstår som en förhållandevis lång tid.

Skälen för regeringens förslag

En europeisk utredningsorder ska kunna avse ett föreläggande om bevarande

I stort sett all typ av gränsöverskridande bevisinhämtning mellan EU-medlemsstaterna i ett pågående straffrättsligt förfarande regleras i lagen om en europeisk utredningsorder. Lagen genomför Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området. Direktivet kräver att en europeisk utredningsorder ska kunna omfatta samtliga utredningsåtgärder som syftar till bevisinhämtning och som finns tillgängliga i nationell rätt (se artikel 3 och skäl 8).

Genom regeringens förslag om att införa en möjlighet till föreläggande om bevarande av vissa uppgifter skapas dels en möjlighet att utfärda en europeisk utredningsorder i Sverige för ett sådant föreläggande, dels en skyldighet att erkänna och verkställa en sådan order från en annan medlemsstat. Åtgärden bör därför tas upp i den paragraf i lagen om en europeisk utredningsorder som anger vilka åtgärder som en europeisk utredningsorder kan avse eller motsvara (se 1 kap. 4 §).

Utfärdande i Sverige av en europeisk utredningsorder för ett föreläggande om bevarande

Utgångspunkten vid utfärdandet av en europeisk utredningsorder är de förutsättningar som gäller för den aktuella utredningsåtgärden enligt svensk rätt (se 2 kap. 3 §). Kraven på bl.a. att uppgiften skäligen kan antas ha betydelse för utredningen, tid för bevarande och vem ett föreläggande får riktas mot i de föreslagna 27 kap. 16 och 16 a §§ rättegångsbalken bör alltså gälla när en europeisk utredningsorder om att bevara en viss lagrad uppgift utfärdas (se även artikel 6.1 i direktivet). Detsamma gäller det proportionalitetskrav som finns i 27 kap. 1 § tredje stycket rättegångsbalken. En europeisk utredningsorder för ett bevarande bör kunna beslutas av en åklagare. Eftersom den nya åtgärden föreslås föras in i 1 kap. 4 § 4 lagen om en europeisk utredningsorder behövs inga särskilda bestämmelser för att åstadkomma detta (se 2 kap. 1 §).

Som föreslås i promemorian behöver de nationella bestämmelserna kompletteras med regler för vad som ska gälla specifikt när en europeisk utredningsorder för att bevara en viss lagrad uppgift utfärdas.

Ett beslut om en europeisk utredningsorder för ett föreläggande om bevarande bör kunna prövas på samma sätt som ett nationellt beslut om åtgärden. Det som sägs om rättens prövning i 27 kap. 6 § första stycket rättegångsbalken ska då gälla.

En europeisk utredningsorder för ett föreläggande om bevarande behöver kunna bestå under den tid som den andra medlemsstaten enligt direktivet har på sig för att erkänna och verkställa dels den ordern, dels en efterföljande order för röjande av uppgifterna. Tiden för bevarande bör därför räknas från verkställighetstidpunkten i den andra medlemsstaten. Det är först då den som har förelagts blir skyldig att vidta åtgärder för att bevara uppgiften.

Direktivets tidsfrister innebär att den verkställande staten har upp till 120 dagar på sig att erkänna och verkställa en mottagen utredningsorder. I

den kompletterande promemorian föreslås därför en möjlighet till förlängning av tiden för bevarande med totalt 90 dagar utöver den ursprungliga fristen om 90 dagar. Regeringen delar promemorians bedömning att en möjlighet till förlängning med totalt 90 dagar bör vara tillräckligt för att ordningen ska vara förenlig med de tidsfrister som framgår av direktivet som lagen om en europeisk utredningsorder bygger på (direktiv 2014/41/EU). I avsnitt 6.1.1 har också behovet av en enhetlig förlängningsfrist redovisats.

JO påpekar att en möjlighet till förlängning av bevarandetiden med totalt 90 dagar framstår som en förhållandevis lång tid. Som konstaterats ovan bör, med hänsyn till de integritetsaspekter som gör sig gällande vid ett föreläggande om bevarande, möjligheten till förlängning bara utnyttjas om det finns särskilda skäl för det. Så kan t.ex. vara fallet i mer komplicerade utredningar där det kan ta tid innan det finns förutsättningar för att utfärda en efterföljande order för röjande av uppgifterna. Ett annat fall där det kan finnas särskilda skäl för en förlängning är om det tar längre tid än beräknat för den andra medlemsstaten att verkställa den efterföljande ordern. Regeringen gör bedömningen att den föreslagna fristens utformning utgör en rimlig avvägning mellan behovet av en effektiv reglering och det integritetsintrång ett bevarande kan innebära för den som drabbas av åtgärden. Jämfört med förslaget i promemorian bör det dock av författningstexten tydligare framgå att förlängningstiden om 90 dagar är en maximitid. Tiden för förlängning bör inte bestämmas till längre än nödvändigt.

Sammantaget föreslår regeringen att en europeisk utredningsorder för ett föreläggande om bevarande ska utfärdas av en åklagare. När den europeiska utredningsordern har verkställts i den andra medlemsstaten ska den som förelagts att bevara en viss lagrad uppgift kunna begära att åtgärden prövas i domstol. Den tid för bevarande om 90 dagar som anges i förslaget till 27 kap. 16 § andra stycket rättegångsbalken ska räknas från verkställighetstidpunkten i den andra medlemsstaten och får förlängas med högst 90 dagar om det finns särskilda skäl.

Erkännande och verkställighet i Sverige av en europeisk utredningsorder för ett föreläggande om bevarande

Erkännande och verkställighet av en europeisk utredningsorder för ett föreläggande om bevarande bör, liksom ett utfärdande, handläggas av åklagaren. Eftersom den nya åtgärden föreslås föras in i 1 kap. 4 § 4 lagen om en europeisk utredningsorder behövs inga särskilda bestämmelser för att åstadkomma det (se 3 kap. 8 §).

Samma förfarande bör användas som när en motsvarande åtgärd beslutas i en svensk förundersökning (se 3 kap. 12 §). Om den europeiska utredningsordern erkänns ska åklagaren meddela en verkställbarhetsförklaring enligt 3 kap. 19 §. Den ska vara skriftlig och bl.a. innehålla uppgift om vilken åtgärd som ska verkställas. Förklaringen ska också innehålla andra uppgifter av betydelse för verkställigheten, t.ex. hur länge de lagrade uppgifterna ska bevaras.

För verkställigheten av en europeisk utredningsorder bör också de förutsättningar som gäller för den aktuella utredningsåtgärden enligt svensk rätt som utgångspunkt tillämpas (se 3 kap. 21 § lagen om en europeisk utredningsorder och artikel 9 i direktivet). Som framhålls i promemorian

kommer det dessutom att behövas en särskild reglering för vissa frågor som rör verkställigheten.

Den som har förelagts att bevara en viss lagrad uppgift bör kunna begära att rätten prövar åklagarens beslut om erkännande och verkställighet av en europeisk utredningsorder för åtgärden. Prövningen ska avse verkställbarhetsförklaringen och inte de sakliga skälen för föreläggandet (se artikel 14.2 i direktivet). För rättens prövning, behörig domstol och effekter av ett upphävande, bör samma regler gälla som för beslag och tillträdesförbud, med vissa undantag (se 3 kap. 32 och 33 §§ lagen om en europeisk utredningsorder).

När Sverige är verkställande stat behöver ett bevarande kunna bestå inte bara under den tid som åklagaren prövar den aktuella utredningsordern, utan också under den tid han eller hon behöver för att pröva om en efterföljande utredningsorder för röjande av uppgifterna ska erkännas och verkställas. Som utgångspunkt gäller, som nämnts, samma förutsättningar för verkställigheten av en europeisk utredningsorder som för den aktuella utredningsåtgärden enligt svensk rätt (se 3 kap. 21 § lagen om en europeisk utredningsorder och artikel 9 i direktivet). Den möjlighet till förlängning med högst 90 dagar som regeringen föreslår kommer därför att gälla även vid verkställighet av en europeisk utredningsorder för ett föreläggande om bevarande (se förslaget till 27 kap. 16 § rättegångsbalken).

JO påpekar att den möjlighet till förlängning med totalt 90 dagar som föreslås i promemorian framstår som en förhållandevis lång tid. Som redan nämnts gäller vissa särskilda förutsättningarna för det rättsliga samarbetet vid en europeisk utredningsorder. Framförallt måste förlängningsmöjligheten ta höjd för direktivets tidsfrister för medlemsstaternas handläggning av erkännande och verkställighet av en utfärdad order (se artikel 12 i direktivet). Precis som vid utfärdande av en europeisk utredningsorder för bevarande bedöms en förlängningsmöjlighet om högst 90 dagar vara en rimlig avvägning mellan behovet av en effektiv reglering och det integritetsintrång ett bevarande kan innebära för den som drabbas av åtgärden. Möjligheten till förlängning med upp till maximalt 90 dagar ska enbart utnyttjas när det på grund av någon särskild omständighet är nödvändigt för att de bevarade uppgifterna inte ska utplånas innan en utredningsorder för en åtgärd om röjande har hunnit verkställas. Så kan t.ex. vara fallet om det tar längre tid än beräknat för den andra medlemsstaten att utfärda den efterföljande utredningsordern. Inte heller vid en förlängning ska tiden bestämmas till längre än nödvändigt. Jämfört med förslaget i promemorian bör möjligheten till förlängning regleras i rättegångsbalken istället för i lagen om en europeisk utredningsorder. Skälen för det redovisas i avsnitt 6.1.1.

Om den andra medlemsstatens myndigheter inte ger in en efterföljande europeisk utredningsorder inom den tid som åklagaren angett i verkställbarhetsförklaringen, eventuellt efter en förlängning, upphör föreläggandet att gälla utan ytterligare åtgärd. Det behövs inte några särskilda regler om det.

Sammanfattningsvis föreslår regeringen att en åklagare ska pröva om en europeisk utredningsorder för ett föreläggande om bevarande ska erkännas och verkställas i Sverige. När den europeiska utredningsordern har verkställts i Sverige ska den som har förelagts att bevara en viss lagrad uppgift kunna begära rättens prövning av verkställbarhetsförklaringen.

Vilka förutsättningar bör gälla vid erkännande och verkställighet?

Ett föreläggande om bevarande är en tvångsåtgärd som med hänsyn till systematiken i lagen om en europeisk utredningsorder bör omfattas av det fakultativa kravet på dubbel straffbarhet i 3 kap. 7 §. Några ytterligare lagstiftningsåtgärder behöver inte vidtas för att åstadkomma det.

Ett föreläggande om bevarande bör inte kunna riktas mot den som skäligen kan misstänkas för brottet eller mot någon till honom eller henne sådan närstående person som avses i 36 kap. 3 § rättegångsbalken (se förslaget till 27 kap. 16 § fjärde stycket rättegångsbalken). En sådan begränsning bör också gälla vid erkännande och verkställighet av en europeisk utredningsorder för ett föreläggande om bevarande, vilket bedöms vara förenligt med direktiv 2014/41/EU (se artikel 1.4 och 11.1 f samt skäl 18 och 19). Det föreslås därför att det av 3 kap. 5 § första stycket 2 ska framgå att förbudet i föreslagna 27 kap. 16 § fjärde stycket rättegångsbalken utgör hinder för erkännande och verkställighet av en europeisk utredningsorder för ett föreläggande om bevarande.

6.2 Röjande av trafikuppgifter (artikel 17 och 30)

6.2.1 En skyldighet att lämna ut information om tillhandahållare som deltagit i överföringen

Regeringens förslag: En tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster ska vara skyldig att på begäran av den myndighet som beslutat om ett föreläggande om bevarande lämna ut uppgift om vilka övriga tillhandahållare som har deltagit vid överföringen av det meddelande som omfattas av föreläggandet.

Tystnadsplikt ska gälla för uppgift som hänför sig till en sådan begäran.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Post- och telestyrelsen* anser att det bör understrykas att bestämmelsen inte innebär ett krav på tillhandahållaren att inskaffa uppgifter och att det bara är sändningsvägarna för en viss kommunikation som ska anges. Post- och telestyrelsen anser även att det är rimligt att tillhandahållarna får ersättning för sina kostnader.

Skälen för regeringens förslag: Ett säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 16 ska vara möjligt oavsett om en eller flera tjänsteleverantörer har deltagit i överföringen (se artikel 17). Det förutsätter att det går att identifiera vilka tjänsteleverantörer som har deltagit i överföringen. Konventionsstaterna ska därför garantera att en tillräcklig mängd sådana trafikuppgifter som avses i artikel 16 skyndsamt ska kunna röjas för myndigheterna så att tjänsteleverantörerna och den väg meddelandet överförts ska kunna identifieras (se artikel 17.1 b). Som *Post- och telestyrelsen* framhåller innefattar bestämmelsen inte något krav på att tillhandahållaren ska inskaffa uppgifter.

Med uttrycket tjänsteleverantör avses 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 (se artikel 1 c).

Utredningen bedömer att möjligheten att snabbt få tillgång till de uppgifter som avses är alltför begränsad i svensk rätt. Regeringen delar den bedömningen. För att göra det möjligt att få tillgång till uppgifterna på ett snabbt och effektivt sätt bör den tillhandahållare som först identifierats av de brottsutredande myndigheterna kunna åläggas att lämna ut trafikuppgifter i den utsträckning som krävs för att fler tillhandahållare i överföringskedjan ska kunna identifieras. I praktiken kommer det huvudsakligen att vara sådana tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster som omfattas av anmälningsplikten i lagen om elektronisk kommunikation som blir aktuella. Genom att begränsa kretsen till dessa aktörer blir det också en möjlig och rimlig uppgift för den som begäran riktas mot att ta fram den efterfrågade informationen.

Tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster som har förelagts att bevara en viss lagrad uppgift bör alltså kunna åläggas att på begäran av den myndighet som beslutat om föreläggandet lämna ut uppgift om vilka övriga tillhandahållare som har deltagit vid överföringen av det meddelande som berörs av föreläggandet. Det föreslås ett tillägg till undantaget från tystnadsplikt i 6 kap. 22 § lagen om elektronisk kommunikation av den innebörden.

Som *Post- och telestyrelsen* påpekar omfattar den föreslagna regleringen endast information om vilka tillhandahållare som deltagit vid en överföring så att ett föreläggande om bevarande kan riktas även mot dessa. Det ska enbart vara möjligt att ta reda på från vilken tillhandahållare som meddelandet sändes och, för det fall det har vidaresänts, till vilken tillhandahållare det vidaresändes. Det ankommer på tillhandahållaren att ta fram de uppgifter som begärs. Om leverantören inte har någon uppgift om vilka de övriga aktörerna är kommer någon information inte att kunna lämnas ut. Förslaget innebär inte heller något nytt krav på att spara eller lagra uppgifter.

Uppgift om vilka övriga tillhandahållare som har deltagit vid överföringen kommer i den övervägande delen av fallen kunna fås fram genom de trafikuppgifter som omfattas av lagringsskyldighet enligt 6 kap. 16 a § lagen om elektronisk kommunikation. Sådana trafikuppgifter får endast behandlas för att lämnas ut enligt vissa bestämmelser som särskilt anges (se 6 kap. 16 c §). De trafikuppgifter som det nu är fråga om bör kunna behandlas för att lämnas ut till den myndighet som har beslutat om ett föreläggande om bevarande. Det föreslås därför att detta uttryckligen ska framgå av lagen. När det gäller *Post- och telestyrelsens* synpunkt om ersättning för kostnader bör bestämmelserna om ersättning för kostnader och om anpassning för utlämnande i 6 kap. 16 e och 16 f §§ även gälla för uppgift om övriga leverantörer som lämnas ut enligt den nya bestämmelsen. Det krävs inga ytterligare ändringar för att åstadkomma detta.

Tillhandahållarna har tystnadsplikt bl.a. för uppgift som hänför sig till användning av vissa hemliga tvångsmedel och för begäran om utlämnande av uppgift om abonnemang vid misstanke om brott (6 kap. 21 §).

Tystnadsplikt bör gälla även för begäran om utlämnande av uppgift om vilka övriga tillhandahållare som deltagit i överföringskedjan av ett meddelande som omfattas av ett föreläggande om bevarande. Ett tillägg om det bör göras i bestämmelsen. Regeringens förslag innebär inte att den föreslagna tystnadsplikten har företräde framför den grundlagsskyddade rätten att meddela och offentliggöra uppgifter.

6.2.2 Det ska vara möjligt att lämna ömsesidig rättslig hjälp med information om tillhandahållare som deltagit i överföringen

Regeringens bedömning: I samband med verkställighet av en ansökan om rättslig hjälp eller en europeisk utredningsorder för ett föreläggande om bevarande bör åklagaren kunna begära att uppgifter om vilka övriga tillhandahållare som har deltagit vid överföringen av ett meddelande lämnas ut. Det krävs inte några ytterligare lagstiftningsåtgärder för att åstadkomma detta.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot bedömningen.

Den kompletterande promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inget att invända mot bedömningen. *Sveriges advokatsamfund* invänder mot bedömningen eftersom det bakomliggande förslaget om röjande av uppgifter om tillhandahållare avstyrks. Om det införs en möjlighet till sådant röjande har samfundet emellertid inget att invända mot promemorians bedömning.

Skälen för regeringens bedömning: De brottsutredande myndigheterna kan vid verkställighet av en framställning om skyndsamt säkrande av trafikuppgifter upptäcka att en tjänsteleverantör i en annan stat har medverkat i överföringen av ett meddelande. Det ska då vara möjligt att snabbt röja den mängd trafikuppgifter som behövs för att identifiera tjänsteleverantören och vägen som meddelandet överförts på för den ansökande staten (se artikel 29 och 30).

En ansökan om att säkra lagrade datorbehandlingsbara uppgifter hos en tjänsteleverantör ska enligt artikel 29 och 30 i Budapestkonventionen automatiskt anses innefatta en skyldighet för den anmodade staten att till den ansökande staten tillhandahålla uppgifter om andra tjänsteleverantörer som har medverkat i överföringen av ett meddelande.

Genom att i lagen om elektronisk kommunikation införa en möjlighet till att skyndsamt kunna lämna ut vissa trafikuppgifter så som föreslagits i avsnitt 6.2.1 ovan, skapas de grundläggande förutsättningarna för att åklagaren ska kunna begära ut informationen även vid verkställighet av ett föreläggande om bevarande i internationella situationer.

Det tillvägagångssätt och de förutsättningar som föreslås gälla nationellt bör även gälla i samband med att en ansökan om rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål eller en europeisk utredningsorder för ett föreläggande om bevarande verkställs i Sverige.

Samma bestämmelser ska tillämpas som när en motsvarande åtgärd verkställs i en svensk förundersökning (se 2 kap 1 § lagen om internationell rättslig hjälp i brottmål och 3 kap. 21 § lagen om en europeisk utredningsorder). När en ansökan om rättslig hjälp eller en europeisk utredningsorder för ett föreläggande om bevarande verkställs och föreläggandet riktar sig mot en tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster som omfattas av lagen om elektronisk kommunikation kan åklagaren därför, i samband med verkställigheten, begära tillgång till uppgifter om vilka andra leverantörer som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande om bevarande (se 6 kap. 22 § första stycket 14 i lagen). Skyldigheten för en tillhandahållare att lämna ut dessa uppgifter förutsätter att det finns ett bakomliggande föreläggande om bevarande. Om ett föreläggande har hävts, t.ex. efter domstolens prövning, är det inte heller möjligt att begära att uppgifter om andra tillhandahållare lämnas ut.

Sammanfattningsvis delar regeringen utredningens och promemorians bedömningar att det ska vara möjligt för åklagaren att i samband med verkställighet av en ansökan om rättslig hjälp eller en europeisk utredningsorder för ett föreläggande om bevarande begära att uppgifter om vilka övriga tillhandahållare som har deltagit vid överföringen av ett meddelande lämnas ut. Det krävs inte några ytterligare lagstiftningsåtgärder för att åstadkomma detta.

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

Regeringens bedömning: Svensk rätt uppfyller konventionens krav om husrannsakan och beslag.
Det bör inte införas någon möjlighet till informationsföreläggande.

Utredningens bedömning och förslag överensstämmer delvis med regeringens bedömning. Utredningen föreslår dock att det i svensk rätt ska införas en specifik möjlighet till föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö (informationsföreläggande).

Remissinstanserna: Ett flertal av remissinstanserna uttalar sig inte särskilt över bedömningen. *Domstolsverket*, *Försvarsmakten, Rättighetsalliansen*, *Stockholms universitet (Juridiska fakulteten)* och *Uppsala universitet (Juridiska fakultetsnämnden)* tillstyrker utredningens förslag. *Ekobrottsmyndigheten* och *Åklagarmyndigheten* tillstyrker utredningens förslag men anser att det bör klarläggas huruvida husrannsakan på distans är rättsligt möjligt. *Helsingborgs tingsrätt, Polismyndigheten* och *Säkerhetspolisen* tillstyrker förslaget men ifrågasätter hur effektiv en sådan åtgärd i praktiken kan bli i brist på sanktionsmöjligheter. *Bahnhof AB*, *Datainspektionen*, *Hovrätten över Skåne och Blekinge* och *Sveriges advokatsamfund* avstyrker förslaget. *Hovrätten för Västra Sverige, Hovrätten över Skåne och Blekinge* och *JO* påtalar riskerna för att ett föreläggande kan komma att strida mot förbudet mot självinkriminering. *Svenska journalistförbundet* och *Sveriges advokatsamfund* anför att förslaget kan komma i konflikt med bestämmelser om sekretess och tystnadsplikt i annan

lagstiftning. *Hovrätten över Skåne och Blekinge* delar utredningens bedömning att de svenska reglerna om vittnesförhör utom rätta redan uppfyller de krav som ställs i artikel 19.4 och påpekar att den analys som görs av behovet talar för att regeln inte skulle få avsedd effekt. *Datainspektionen* ser stora integritetsrisker med förslaget. *Sveriges advokatsamfund* har synpunkter på den proportionalitetsavvägning som ligger till grund för förslaget. *Bahnhof AB, Hovrätten över Skåne och Blekinge*, *Juliagruppen*, *Lunds universitets internetinstitut, Sveriges advokatsamfund* och *Internetstiftelsen* framhåller att förslaget kan medföra lojalitetskonflikter för den som har förelagts.

Skälen för regeringens bedömning

Svensk rätt uppfyller konventionens krav om husrannsakan

De brottsutredande myndigheterna ska genom husrannsakan eller på annat sätt kunna bereda sig tillgång till ett datorsystem, en del därav eller ett annat medium för lagring av datorbehandlingsbara uppgifter och de uppgifter som finns lagrade där (se artikel 19).

En husrannsakan får 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 utredningen om brottet eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken (se 28 kap. 1 § rättegångsbalken). Befogenheten för de brottsutredande myndigheterna att vid en husrannsakan söka efter uppgifter som finns lagrade i datorer är inte uttryckligen reglerad. Den allmänna uppfattningen är dock att det inte finns något hinder mot att söka efter lagrad information i en dator som påträffas under en husrannsakan (se t.ex. propositionen Hemlig dataavläsning, prop. 2019/20:64 s. 75).

Enligt konventionen ska det vidare vara möjligt att skyndsamt utvidga en undersökning av ett datorsystem till ett annat datorsystem eller del därav (se artikel 19.2). 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 (se den förklarande rapporten till konventionen p. 194).

En utvidgad undersökning av ett tillkommande datorsystem kan således redan i dag göras med stöd av de svenska reglerna om husrannsakan. I de flesta fall kan husrannsakan dessutom ske utan förordnande av rätten. Det finns därför förutsättningar för en åklagare eller en annan undersökningsledare att 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.

Regeringen delar utredningens bedömning att svensk rätt uppfyller kraven i artikel 19.1 och 2 genom bestämmelserna om husrannsakan. Husrannsakan kan användas vid samtliga brott som anges i artikel 14.2 och de begränsningar som svensk rätt uppställer när det gäller bl.a. brottets allvar och proportionalitet får anses vara godtagbara mot bakgrund av den proportionalitetsprincip som kommer till uttryck i artikel 15. När det gäller det av *Åklagarmyndigheten* och *Ekobrottsmyndigheten* efterfrågade klarläggandet huruvida husrannsakan på distans är rättsligt möjligt har frågan om undersökning av elektronisk information på distans övervägts av Beslagsutredningen (se betänkandet Beslag och husrannsakan – Ett regelverk

för dagens behov, SOU 2017:100 s. 279). Utredningens förslag har remitterats och bereds för närvarande i Regeringskansliet.

Hanteringen av säkrad information

De brottsbekämpande myndigheterna ska ha rätt att beslagta eller på liknande sätt säkra datorbehandlingsbara uppgifter som har åtkommits enligt punkterna 1 och 2 i artikel 19 (se artikel 19.3). Myndigheternas närmare befogenheter anges i punkterna a–d.

Det är möjligt att med stöd av de allmänna bestämmelserna om beslag i 27 kap. rättegångsbalken beslagta datorer, mobiltelefoner och andra bärare av datorbehandlingsbara uppgifter. Det innebär att det i och för sig är möjligt att säkra datorbehandlingsbara uppgifter på det sätt som anges i artikel 19.3. Utredningen har övervägt om det förbud som finns mot beslag i vissa fall skulle innebära ett hinder för tillämpningen av reglerna som inte är förenligt med konventionens krav (se också NJA 2015 s. 631 angående beslagsförbudet och bärare av datorbehandlingsbara uppgifter). Regeringen delar utredningens bedömning att den begränsning beslagsförbudet innebär inte utgör ett sådant hinder mot bakgrund av rättighetsskyddet i artikel 15.

Artikeln ställer krav på att det ska finnas en möjlighet att framställa och behålla en kopia av uppgifterna. Det är vanligt att brottsutredande myndigheter i Sverige kopierar beslagtaget material, både fysiska skriftliga handlingar och elektronisk information som lagrats i datorer. Förfarandet är oreglerat. Regeringen anser, liksom utredningen, att någon uttrycklig reglering inte krävs för att uppfylla konventionens krav. Det räcker att det finns en faktisk möjlighet att kopiera uppgifterna och bevara kopian. Frågan om kopiering bör införas som ett särskilt tvångsmedel har övervägts av Beslagsutredningen (se betänkandet Beslag och husrannsakan – ett regelverk för dagens behov, SOU 2017:100 s. 393 och 410). I betänkandet görs ingen annan bedömning av svensk rätts förenlighet med Budapestkonventionen i denna del.

Sammanfattningsvis bedömer regeringen att det inte krävs några lagstiftningsåtgärder för att uppfylla kraven om hantering av information som åtkommits genom husrannsakan i artikel 19.3.

Det bör inte införas någon möjlighet till informationsföreläggande

Det ska vara möjligt att förelägga en person som har kunskap om ett datorsystems funktion att i den mån det är skäligt lämna information som är nödvändig för att möjliggöra husrannsakan enligt punkterna 1 och 2 i artikel 19 (se artikel 19.4).

Förundersökningsledaren kan kräva att det hålls vittnesförhör inför rätta under en förundersökning (23 kap. 13 § rättegångsbalken). Samma skyldighet för ett vittne att uttala sig gäller då som vid ett vanligt vittnesförhör. Ett sådant förhör förutsätter 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 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.

Utredningen gör bedömningen att en målsägande som drabbas av husrannsakan antingen själv eller genom ombud får förutsättas frivilligt lämna 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 målsäganden anses därför inte finnas. Det kan aldrig bli fråga om att utfärda ett informationsföreläggande mot en misstänkt mot bakgrund av artikel 6 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och förbudet mot självinkriminering i FN:s konvention om medborgerliga och politiska rättigheter. Att dessa rättigheter ska beaktas vid tillämpningen av Budapestkonventionens bestämmelser framgår av ingressen. När det gäller att få information från någon som vare sig är målsägande eller misstänkt anser utredningen att möjligheten att hålla vittnesförhör inför rätta enligt 23 kap. 13 § rättegångsbalken bör vara ett tillräcklig effektivt medel. Enligt utredningen uppfyller således svensk rätt kraven i artikel 19.4.

Trots slutsatsen att svensk rätt uppfyller konventionskraven i detta hänseende föreslår utredningen att en ny bestämmelse om informationsföreläggande ska införas i 28 kap. rättegångsbalken. Enligt förslaget ska en person med kunskap om ett datorsystems funktion kunna föreläggas att lämna information som är nödvändig för att möjliggöra husrannsakan. Förslaget motiveras huvudsakligen med att de brottsutredande myndigheterna uppgett att det finns ett stort praktiskt behov av åtgärden.

Hovrätten för Västra Sverige ifrågasätter utredningens bedömning att svensk rätt redan uppfyller kraven i artikel 19.4 eftersom möjligheten att hålla vittnesförhör under förundersökningen förutsätter att det finns någon som är skäligen misstänkt. Artikel 19.4 innehåller inga sådana begränsningar och i en förundersökning kan behov av nu aktuell information uppkomma redan innan det finns någon som är skäligen misstänkt. Andra remissinstanser, däribland *Stockholms universitet (Juridiska fakulteten)*, delar utredningens bedömning att svensk rätt redan uppfyller konventionens krav.

Artikel 19.4 anger att parterna ska bemyndiga sina behöriga myndigheter att förelägga en person att i den mån det är skäligt lämna viss information. Avgränsningen av möjligheten att hålla vittnesförhör inför rätta enligt 23 kap. 13 § rättegångsbalken till situationer där det finns någon som är skäligen misstänkt vilar på en sådan skälighetsavvägning. Av förarbetena framgår att begränsningen infördes bl.a. på grund av farhågan att det annars skulle föreligga en fara för att förhöret kan ledas i en viss riktning och att vittnena kan komma att avge ensidiga utsagor vilka de sedan vid huvudförhandlingen, inför hotet om ansvar för mened, inte vågar rätta. Vidare skulle det utan begränsningen kunna ifrågasättas om inte vittnesförhör kan begäras med den som misstänktes för brottet (se NJA II 1943 s. 310).

Mot den bakgrunden bedömer regeringen att avgränsningen av möjligheten att hålla vittnesförhör inför rätta till situationer där det finns någon som är skäligen misstänkt är förenlig med den möjlighet till begränsning som finns i artikel 19.4. Sammanfattningsvis uppfyller svensk rätt alltså konventionens krav om husrannsakan och beslag, huvudsakligen genom befintliga bestämmelser om husrannsakan, beslag och vittnesförhör inför rätta under en förundersökning.

Regeringen konstaterar att ett flertal av de remissinstanser som yttrar sig över förslaget om att införa en möjlighet till informationsföreläggande, bl.a. *Svenska journalistförbundet*, *JO*, *Hovrätten över Skåne och Blekinge* och *Sveriges advokatsamfund*, har invändningar om källskydd, lojalitetskonflikter, integritetsintrång och risk för självinkriminering. Även om ett flertal remissinstanser, bl.a. *Åklagarmyndigheten* och *Säkerhetspolisen*, har tillstyrkt förslaget finns det också skäl som talar emot det. Regeringen bedömer att det inte finns tillräckliga skäl för att gå vidare med förslaget om informationsföreläggande med hänsyn till de farhågor som har lyfts och till att det inte heller är nödvändigt för att uppfylla konventionens krav. Det bör alltså inte införas någon möjlighet till informationsföreläggande.

6.4 Vilka förbehåll behöver Sverige göra?

I avsnittet behandlas frågan om vilka förbehåll Sverige behöver göra. Några frågor om förbehåll diskuteras dock, av pedagogiska skäl, i anslutning till behandlingen av aktuell artikel. Behovet av förbehåll för att kunna vägra rättslig hjälp med ett föreläggande om bevarande i vissa fall (artikel 29.4) har diskuterats i avsnitt 6.1.2. Att det inte finns något behov av förbehåll för att uppfylla konventionens krav på kriminalisering av medhjälp och försökt till brott (artikel 11.3) behandlas i avsnitt 7.1.

6.4.1 Insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter

Regeringens förslag: Sverige ska avge en förklaring om att Sverige förbehåller sig rätten att endast tillämpa insamling i realtid av trafikuppgifter på de brott och brottstyper som avses i 27 kap. 19 § tredje stycket rättegångsbalken. Sverige ska också avge en förklaring om att Sverige förbehåller sig rätten att inte tillämpa insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter på meddelanden som överförs inom en tjänsteleverantörs datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna tillstyrker eller har inget att invända mot förslaget.

Skälen för regeringens förslag

Förbehåll i fråga om insamling

Det står varje fördragsslutande stat fritt att avgöra vid vilka brott avlyssning av innehållsuppgifter ska kunna användas (se artikel 21). Insamling i realtid av trafikuppgifter ska som huvudregel vara möjligt vid utredningar av dels brott enligt 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 20 och särskilt hänvisningen i punkt 4 till artikel 14).

En fördragsslutande stat får förbehålla sig rätten att endast tillåta insamling i realtid av trafikuppgifter för brott eller brottstyper som anges i

förbehållet. Ett sådant förbehåll förutsätter att omfattningen av dessa brott eller brottstyper inte är mer begränsad än de brott på vilka staten tillåter avlyssning av innehållsuppgifter (se artikel 14.3 a).

Insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter är i svensk rätt möjligt genom hemlig övervakning och avlyssning av elektronisk kommunikation (se 27 kap. 18–20 §§ rättegångsbalken). Dessa tvångsmedel kan användas för att samla in sådana trafikuppgifter (dvs. uppgifter om ett meddelandes ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av tjänst) som avses i artikel 20 och för att ta upp innehållsuppgifter på det sätt som avses i artikel 21.

Eftersom det står varje fördragsslutande stat fritt att avgöra vid vilka brott avlyssning av innehållsuppgifter ska kunna användas är de svenska reglerna förenliga med konventionens krav, även om sådan avlyssning endast kan användas i en förundersökning om brott med högt straffminimum eller straffvärde.

När det däremot gäller insamling i realtid av trafikuppgifter kan det svenska tvångsmedlet hemlig övervakning av elektronisk kommunikation inte användas för att utreda samtliga brott i konventionens straffrättsliga del. Tvångsmedlet får endast användas vid en förundersökning om vissa särskilt angivna brott (se 27 kap. 19 § tredje stycket rättegångsbalken). Regeringen anser i likhet med utredningen att begränsningen i 27 kap. 19 § tredje stycket innebär att Sverige bör lämna förbehåll i enlighet med artikel 14.3 a och att svensk rätt uppfyller artikelns förutsättningar för att lämna ett sådant förbehåll.

Sverige bör därmed förbehålla sig rätten att endast tillämpa de åtgärder som avses i artikel 20 på de brott och brottstyper som avses i 27 kap. 19 § tredje stycket rättegångsbalken.

Förbehåll för meddelanden i vissa kommunikationsnät

Hemlig övervakning och avlyssning av elektronisk kommunikation får 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 (se 27 kap. 20 § tredje stycket rättegångsbalken). Syftet med regeln är att från tvångsmedlens tillämpningsområde undanta områden för elektronisk kommunikation som är särskilt integritetskänsliga eller som annars får anses tillhöra den privata sfären (se propositionen Hemlig teleavlyssning och hemlig teleövervakning, prop. 1994/95:227 s. 27).

Det finns en möjlighet för en fördragsslutande stat att förbehålla sig rätten att inte tillämpa insamling i realtid av trafikuppgifter eller avlyssning av innehållsuppgifter 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 (se artikel 14.3 b).

Om möjligheten till förbehåll utnyttjas, krävs ingen ändring av begränsningsregeln i 27 kap. 20 § tredje stycket rättegångsbalken för att uppfylla konventionens krav. De områden för elektronisk kommunikation som är särskilt integritetskänsliga eller som annars får anses tillhöra den privata sfären kan därför vara fortsatt undantagna från regelns

tillämpningsområde. Sverige bör med stöd av artikel 14.3 b 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 är anslutet till ett annat datorsystem.

Konventionen innehåller vidare krav på tystnadsplikt för information som hänför sig till insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter (se artikel 20.3 och 21.3). Regeringen delar utredningens bedömning att bestämmelserna om tystnadsplikt för leverantörer i lagen om elektronisk kommunikation redan omfattar tystnadsplikt för information som hänför sig till insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter (se 6 kap. 21 § i lagen).

Om förbehåll lämnas i de avseenden som nu föreslagits kommer Sverige sammanfattningsvis att uppfylla kraven i artiklarna 20 och 21 utan att några lagstiftningsåtgärder behöver vidtas.

6.4.2 Vissa handlingar ska vara kriminaliserade endast om de begås med uppsåt att uppmuntra till hat, diskriminering eller våld mot folkgrupp

Regeringens förslag: Sverige ska avge en förklaring om att Sverige förbehåller sig rätten att i nationell rätt uppställa krav på att ett förnekande eller ett grovt förringande måste göras 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 förstnämnda karaktäristika för att sådana gärningar som avses i artikel 6.1 ska vara kriminaliserade.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Hässleholms tingsrätt* och *Stockholms universitet (Juridiska fakulteten)* anser att Sverige, enligt vad som föreslogs i Ds 2005:6, bör utnyttja möjligheten att göra ett förbehåll enligt artikel 6.2 b i tilläggsprotokollet. Stockholms universitet (Juridiska fakulteten) anför att relevanta svenska straffbestämmelser inte omfattar de gärningar som avses i artikel 6 och det framstår från yttrandefrihetssynpunkt som viktigt att Sverige inte gör kriminaliseringsåtaganden som det inte finns täckning för.

Skälen för regeringens förslag: Tilläggsprotokollets bestämmelser kräver att de fördragsslutande parterna kriminaliserar 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 och vissa internationella domstolar utgör folkmord eller brott mot mänskligheten (se artikel 6.1).

En fördragsslutande stat får uppställa krav på att ett förnekande eller ett 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, nationellt eller etniskt ursprung liksom även

trosbekännelse, om den används som svepskäl för någon av de förstnämnda utmärkande egenskaperna (se artikel 6.2 a). En part får också förbehålla sig rätten att helt eller delvis avstå från att straffbelägga de gärningar som avses i artikel 6.1 (se artikel 6.2 b).

De gärningar som tilläggsprotokollet kriminaliserar motsvaras huvudsakligen av brottsbalkens bestämmelser om uppvigling och hets mot folkgrupp (16 kap. 5 och 8 §§ brottsbalken). Straffansvaret för hets mot folkgrupp kan tillämpas på ett förnekande eller ett grovt förringande av om gärningen hotar eller uttrycker missaktning för en folkgrupp med anspelning på vissa grunder av det slag som anges i artikel 6.2 b. Sverige bör därför utnyttja den möjlighet som finns att uppställa ytterligare rekvisit för att kriminalisera de handlingar som beskrivs i artikeln.

Mot den bakgrunden delar regeringen utredningens bedömning att Sverige med stöd av artikel 6.2 a bör avge en förklaring om att Sverige förbehåller sig möjligheten att i nationell rätt uppställa krav på att ett förnekande eller ett grovt förringande måste göras 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 förstnämnda karaktäristika, för att sådana gärningar som avses i artikel 6.1 ska vara kriminaliserade.

6.4.3 Det behövs inte något särskilt förbehåll för den svenska särregleringen av tryck- och yttrandefrihetsbrott

Regeringens bedömning: Svensk rätt uppfyller kraven i bestämmelserna om spridande av material och om kränkning i artikel 3 och 5 i tilläggsprotokollet. Något förbehåll behöver inte lämnas.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna delar eller har inget att invända mot bedömningen. *Hässleholms tingsrätt* och *Stockholms universitet (Juridiska fakulteten)* anser att möjligheten att göra förbehåll för den särskilda ansvarsordningen som gäller för tryck- och yttrandefrihetsbrott bör utnyttjas för att garantera den svenska särregleringen även i framtiden.

Skälen för regeringens bedömning: De konventionsslutande parterna ska straffbelägga uppsåtlig och orättmätig spridning eller annat tillgängliggörande av rasistiskt och främlingsfientligt material till allmänheten med hjälp av ett datorsystem (se artikel 3.1). Begreppet tillgängliggöra ska 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). Vad som utgör rasistiskt och främlingsfientligt material definieras i artikel 2.1. En fördragsslutande part får förbehålla sig möjligheten att inte införa straffansvar när det material som avses i artikel 3.1 förespråkar, främjar eller uppmuntrar diskriminering utan samband med hat eller våld, om det finns andra effektiva åtgärder att tillgå (se artikel 3.2). En fördragsslutande stat får också förbehålla sig rätten att inte föreskriva vare sig straffansvar eller andra effektiva åtgärder

för vissa fall av sådan diskriminering om etablerade principer om yttrandefrihet i statens rättssystem hindrar det (se artikel 3.3).

Parterna ska också göra det straffbart att uppsåtligen och orättmätigt, med hjälp av ett datorsystem, offentligt kränka en grupp personer eller en person av det skälet att de tillhör en grupp som utmärks av ras, hudfärg, härstamning, nationellt eller etniskt ursprung liksom även trosbekännelse, om den används som svepskäl för någon av de förstnämnda utmärkande egenskaperna (se artikel 5.1). Bestämmelsen erbjuder samma möjligheter till förbehåll som artikel 3 (se artikel 5.2).

Som utredningen konstaterar innefattar straffbestämmelserna om förtal, uppvigling och hets mot folkgrupp samtliga dessa gärningar (se 5 kap. 1 § samt 16 kap. 5 och 8 §§ brottsbalken). Eftersom brotten även är straffbara som tryck- och yttrandefrihetsbrott när de begåtts i ett grundlagsskyddat medium uppfyller Sverige konventionens krav utan att göra förbehåll i någon del (se 7 kap. 3, 5 och 6 §§ tryckfrihetsförordningen och 5 kap. 1 § yttrandefrihetsgrundlagen). Svensk rätt uppfyller alltså kraven i bestämmelserna om spridande av material och om kränkning i artikel 3 och 5 i tilläggsprotokollet. Något förbehåll, som *Hässleholms tingsrätt* och *Stockholms universitet (Juridiska fakulteten*) efterfrågar, bör mot denna bakgrund inte göras.

7 Det behövs inte några lagändringar för att genomföra de straffrättsliga bestämmelserna

7.1 Konventionens krav på kriminalisering

Regeringens bedömning: Svensk rätt uppfyller konventionens krav på kriminalisering.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna delar eller har inget att invända mot bedömningen. *Barnombudsmannen, Brottsförebyggande rådet* och *ECPAT Sverige* anser att artikel 9 täcker in ett större område än bestämmelsen om barnpornografibrott i 16 kap. 10 a § brottsbalken. *Hovrätten över Skåne och Blekinge* påpekar att det kan finnas anledning att ytterligare reflektera över om förberedelse till brytande av post- eller telehemlighet är tillräckligt kriminaliserat i svensk rätt för att uppfylla kraven i konventionen. *Rättighetsalliansen* ifrågasätter om de befintliga straffrättsliga bestämmelserna i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk är effektiva och föreslår att det införs ett grovt brott i upphovsrättslagen för de fall som omfattas av artikel 10. *Stockholms universitet (Juridiska fakulteten)* efterfrågar en närmare analys av hur artiklarna 3 och 6 ska förstås och hur relevanta svenska straffbestämmelser förhåller sig till dem. De anser också, liksom *Uppsala universitet (Juridiska fakultetsnämnden),* att artikel 7 i konventionen täcker in fler situationer än bestämmelsen om urkundsförfalskning i 14 kap. 1 § brottsbalken

på grund av kravet på en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt.

Skälen för regeringens bedömning

Olagligt intrång (artikel 2 i konventionen)

Uppsåtligt och orättmätigt intrång i hela eller en del av ett datorsystem ska vara straffbart (se artikel 2). Det får uppställas 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.

Den svenska dataintrångsbestämmelsen straffbelägger bl.a. den som uppsåtligen och olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling (se 4 kap. 9 c § brottsbalken). Såväl dataintrångsbestämmelsen som artikel 2 förutsätter alltså att gärningen begås med uppsåt.

Artikeln överensstämmer i huvudsak med artikel 3 i Europaparlamentets och rådets direktiv 2013/40/EU. Vid genomförandet av direktivet ansågs svensk rätt uppfylla den aktuella artikeln i direktivet (prop. 2013/14:92 s. 11–13).

Regeringen delar utredningens bedömning att svensk rätt uppfyller konventionens krav på kriminalisering av olagligt dataintrång genom befintliga straffbestämmelser.

Olaglig avlyssning (artikel 3 i konventionen)

Det ska 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 (se artikel 3). Krav får uppställas på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Det som konventionen betecknar som olaglig avlyssning kan utgöra brytande av telehemlighet, om det är fråga om överföring av meddelanden via ett allmänt kommunikationsnät, med viss reservation för meddelanden som befordras via radio (4 kap. 8 § brottsbalken). Förfarandet kan annars utgöra dataintrång bestående i att någon bereder sig tillgång till uppgifter avsedda för automatiserad behandling, även här med viss reservation för avlyssning av överföring genom radiovågor (4 kap. 9 c § brottsbalken).

Konventionen ställer endast krav på straffbeläggande av avlyssning som sker orättmätigt. I det begreppet ligger att handlandet inte är tillåtet enligt nationell rätt (se den förklarande rapporten p. 38). Ett handlande som är tillåtet enligt etablerade principer i ett land, t.ex. principen om eterns frihet, är i linje med det inte orättmätigt och omfattas därmed inte av kriminaliseringsåtagandet.

Artikeln överensstämmer i huvudsak med artikel 6 i direktiv 2013/40/EU. Vid genomförandet av direktivet ansågs svensk rätt uppfylla den aktuella artikeln i direktivet (prop. 2013/14:92 s. 12–13).

Sammanfattningsvis delar regeringen utredningens bedömning att svensk rätt uppfyller konventionens krav på kriminalisering av olaglig avlyssning genom befintliga straffbestämmelser.

Datastörning (artikel 4 i konventionen)

Det ska vara straffbart att uppsåtligen och orättmätigt skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter (se artikel 4). Krav får uppställas på att handlandet medfört allvarlig skada.

De förfaranden som beskrivs i artikel 4 motsvarar huvudsakligen det svenska brottet dataintrång men kan i vissa fall även tänkas motsvara andra brott, t.ex. skadegörelse och sabotage (12 kap. 1, 2 och 3 §§ och 13 kap. 4–5 §§ brottsbalken).

Artikeln överensstämmer i huvudsak med artikel 5 i direktiv 2013/40/EU. Vid genomförandet av direktivet ansågs svensk rätt uppfylla den aktuella artikeln i direktivet (prop. 2013/14:92 s. 11–13).

Regeringen delar utredningens bedömning att svensk rätt uppfyller konventionens krav på kriminalisering av datastörning genom befintliga straffbestämmelser.

Systemstörning (artikel 5 i konventionen)

Det ska vara straffbart som systemstörning att uppsåtligen och orättmätigt allvarligt hindra ett datorsystems drift genom att mata in, överföra, skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter (se artikel 5).

De förfaranden som beskrivs i artikel 5 motsvarar huvudsakligen det svenska brottet dataintrång.

Artikeln överensstämmer i huvudsak med artikel 4 i direktiv 2013/40/EU. Vid genomförandet av direktivet ansågs svensk rätt uppfylla den aktuella artikeln i direktivet (prop. 2013/14:92 s. 11–13).

Regeringen delar utredningens bedömning att svensk rätt uppfyller konventionens krav på kriminalisering av systemstörning genom befintliga straffbestämmelser.

Missbruk av apparatur (artikel 6 i konventionen)

De konventionsslutande staterna ska straffbelägga uppsåtlig och orättmätig befattning av visst slag med vissa föremål. Med befattning av visst slag avses att tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra. Med vissa föremål avses en apparat vari ingår ett datorprogram som är skapat eller anpassat främst för att begå något av brotten enligt artiklarna 2–5, eller ett datorlösenord, en åtkomstkod eller liknande datorbehandlingsbara uppgifter som kan ge åtkomst till hela eller delar av ett datorsystem med uppsåt att det eller den ska användas för begå något av brotten i artiklarna 2–5 (se artikel 6.1 a). Parterna ska också straffbelägga innehav av ett sådant föremål om det innehas med uppsåt att användas för att begå något av brotten enligt artiklarna 2–5 (se artikel 6.1 b).

Att ta befattning med apparatur eller verktyg på det sätt som beskrivs i artikeln kan enligt svensk rätt utgöra förberedelse till brott enligt 23 kap. 2 § brottsbalken. I förarbetena till bestämmelsen uttalas att den omfattar befattning både med föremål, immateriella rättigheter och med

information som sammanställts på visst sätt. Lagstiftningen ska också kunna komma att täcka sådana hjälpmedel som kan aktualiseras med anledning av den framtida tekniska utvecklingen samt nya former av brottslighet (se propositionen Förberedelse till brott m.m., prop. 2000/01:85 s. 40 f).

Artikeln överensstämmer delvis med artikel 7 i direktiv 2013/40/EU. Vid genomförandet av direktivet ansågs svensk rätt uppfylla den aktuella artikeln i direktivet (prop. 2013/14:92 s. 13).

Regeringen delar utredningens bedömning att de befattningar som ska vara kriminaliserade enligt artikel 6.1 a och b (dvs. tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra samt inneha i syfte att begå brott) motsvarar de förfoganden som är straffbelagda som förberedelse enligt 23 kap. 2 § första stycket 2 brottsbalken. Förberedelse till de brott som i svensk rätt motsvarar artiklarna 2–5 (brytande av telehemlighet genom ett visst angivet förfarande, dataintrång, grov skadegörelse och sabotage) är kriminaliserat (se 4 kap. 9 b och 10 §§, 12 kap. 5 § och 13 kap. 12 § brottsbalken).

Hovrätten över Skåne och Blekinge påpekar att brottet förberedelse till brytande av telehemlighet endast omfattar mycket specifik befattning med det tekniska hjälpmedlet. Regeringen bedömer emellertid att den svenska straffrättsliga regleringen oavsett detta i sin helhet täcker det område som avses i artikel 6. Ett handlande som faller utanför tillämpningsområdet för den särskilda bestämmelsen om förberedelse till brytande av telehemlighet kan istället, beroende på omständigheterna, vara straffbart som förberedelse till något av de andra brott som nämnts. Det är också möjligt att vissa förfaranden kan vara straffbara som medverkan till brott (se 23 kap. 4 § brottsbalken).

Sammantaget bedömer regeringen att svensk rätt uppfyller konventionens krav på kriminalisering av missbruk av apparatur genom befintliga straffbestämmelser.

Datorrelaterad förfalskning (artikel 7 i konventionen)

De konventionsslutande staterna ska straffbelägga gärningar som består i att någon matar in, ändrar, raderar eller undertrycker datorbehandlingsbara uppgifter så att icke autentiska uppgifter uppstår, om det sker uppsåtligt och orättmätigt (se artikel 7). För straffansvar krävs 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. Parterna får uppställa krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar ska gälla.

Mot bakgrund av en den förklarande rapporten är det klart att de uppgifter som avses i artikel 7 är uppgifter som på något sätt har juridisk relevans och att kravet på autenticitet innebär att dokumentet ska kunna knytas till utställaren (se den förklarande rapporten p. 81–85). I den svenska straffbestämmelsen om urkundsförfalskning uttrycks detta istället som att uppgifterna ska ha betydelse som bevis och att de har en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt (14 kap. 1 § brottsbalken). Bestämmelsen erhöll sin nuvarande utformning den 1 juli 2013. I IT-förfalskningsutredningens betänkande som föregick lagstiftningen angavs särskilt att artikel 7 i Budapestkonventionen hade beaktats (se betänkandet

Urkunden i tiden – en straffrättslig anpassning, SOU 2007:92 s. 11). Den proposition som regeringen överlämnade till riksdagen i lagstiftningsärendet överensstämmer i huvudsak med IT-förfalskningsutredningens förslag (se propositionen Förfalsknings- och sanningsbrotten, prop. 2012/13:74).

Även om rekvisiten i de båda bestämmelserna är formulerade på olika sätt bedömer regeringen, till skillnad från *Stockholms universitet (Juridiska fakulteten)* och *Uppsala universitet (Juridiska fakultetsnämnden)*, att tillämpningsområdet i praktiken är detsamma. Svensk rätt bedöms alltså uppfylla konventionens krav på kriminalisering av datorrelaterad förfalskning genom befintliga straffbestämmelser.

Datorrelaterat bedrägeri (artikel 8 i konventionen)

Det ska vara straffbart 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 (se artikel 8).

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 automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan döms för bedrägeri, s.k. datorbedrägeri (se 9 kap. 1 § andra stycket brottsbalken).

Regeringen delar utredningens bedömning att svensk rätt uppfyller konventionens krav på kriminalisering av datorrelaterat bedrägeri genom befintliga straffbestämmelser.

Brott som hänför sig till barnpornografi (artikel 9 i konventionen)

Olika former av befattning med barnpornografi ska vara straffbart när gärningen begås uppsåtligen och orättmätigt (se artikel 9). Med barnpornografi avses material som visuellt avbildar minderåriga på vissa, däri närmare angivna sätt. Begreppet minderårig innefattar alla personer under arton år.

I 16 kap. 10 a § brottsbalken anges vilka handlingar som enligt svensk rätt utgör barnpornografibrott. I bestämmelsen används begreppet barn istället för minderårig. Med barn avses en person vars pubertetsutveckling inte är fullbordad eller som är under arton år. Att skildra någon som är under arton år i pornografisk bild är alltid straffbelagt. För att kunna döma till ansvar för övriga handlingar som räknas upp i paragrafen krävs att den avbildade personens pubertetsutveckling inte är fullbordad eller att det av bilden och omständigheterna kring den framgår att den avbildade personen är under arton år (se 16 kap. 10 a § tredje stycket).

Regeringen delar utredningens bedömning att det i praktiken inte föreligger någon diskrepans mellan vad som ska vara straffbart enligt artikel 9 och vad som är kriminaliserat enligt svensk rätt. Svensk rätt bedöms alltså uppfylla konventionens krav på kriminalisering av brott som hänför sig till barnpornografi genom befintliga straffbestämmelser.

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

Olika former av intrång i upphovsrätt och till upphovsrätten närstående rättigheter ska straffbeläggas, om de begås uppsåtligen, i kommersiell skala och med hjälp av ett datorsystem (se artikel 10). Ideella rättigheter är undantagna från tillämpningsområdet. De upphovsrätter som avses i artikeln anges genom en hänvisning till vissa internationella överenskommelser på upphovsrättens område. 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 partens internationella förpliktelser enligt de nämnda överenskommelserna (se artikel 10.3).

Sverige har tillträtt samtliga internationella överenskommelser som anges i artikeln. De straffrättsliga bestämmelser och andra sanktionsregler som dessa överenskommelser kräver finns i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk. Enligt lagen ska den som uppsåtligen eller av grov oaktsamhet på olika sätt, exempelvis med hjälp av ett datorsystem, gör intrång i en upphovsrätt eller i en till upphovsrätten närstående rättighet dömas för upphovsrättsbrott. Om brottet begåtts uppsåtligen och är att anse som grovt döms för grovt upphovsrättsbrott. Vid bedömningen av om ett brott är grovt ska det särskilt beaktas om gärningen har föregåtts av särskild planering, har utgjort ett led i en brottslighet som utövats i organiserad form, har varit i större omfattning, eller annars har varit av särskilt farlig art. 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 (se 7 kap.). Att ett intrång skett i kommersiell skala är dock en omständighet som kan beaktas i försvårande riktning inom ramen för de nyss angivna kvalifikationsgrunderna.

Regeringen, som också tar i beaktande att det sedan den 1 september 2020 införts en särskild straffskala för de allvarligaste fallen av upphovsrättsintrång i upphovsrättslagen, delar utredningens bedömning att svensk rätt uppfyller konventionens krav på kriminalisering av brott som hänför sig till intrång i upphovsrätt och till upphovsrätten närstående rättigheter genom befintliga sanktionsbestämmelser i lagen om upphovsrätt till litterära och konstnärliga verk.

Medhjälp och försök (artikel 11)

Medhjälp till brotten i artiklarna 2–10 och försök till brott enligt artiklarna 3–5, 7, 8 samt 9.1 a och c i konventionen ska vara straffbelagt (se artikel 11).

Svensk rätt uppfyller konventionens krav på kriminalisering av brotten i artiklarna 2–10. Straffansvar för medhjälp ådöms inte bara den som utfört dessa gärningar utan även annan som har främjat dem med råd eller dåd. De svenska reglerna om ansvar för medhjälp gäller vid alla brottsbalksbrott samt de brott i specialstraffrätten för vilka fängelse är föreskrivet eller för vilka särskild föreskrift finns att medverkan ska bestraffas (se 23 kap. 4 § brottsbalken).

Försök till brott är kriminaliserat i de fall det särskilt anges (se 23 kap. 1 § brottsbalken). Försök till de brott i svensk lagstiftning som motsvarar

brott enligt artiklarna 3–5, 7, 8 samt 9.1 a och c är kriminaliserat med undantag för brytande av telehemlighet (se 4 kap. 10 §, 9 kap. 11 §, 12 kap. 5 §, 13 kap. 12 §, 14 kap. 13 § och 16 kap. 17 § brottsbalken). Liksom utredningen anser regeringen emellertid att straffbestämmelsen om förberedelse i 4 kap. 9 b § brottsbalken uppfyller konventionens krav på kriminalisering av samtliga stadier före fullbordat brott av brytande av telehemlighet. Det finns därför ingen anledning att utnyttja möjligheten till förbehåll i artikel 11.3.

Regeringen delar sammanfattningsvis utredningens bedömning att svensk rätt uppfyller konventionens krav i bestämmelsen om medhjälp och försök genom brottsbalkens bestämmelser om medhjälp, förberedelse och försök till brott.

Juridiska personers ansvar (artikel 12 i konventionen)

Även juridiska personer ska kunna hållas ansvariga för brott enligt konventionen (se artikel 12). Det står en fördragsslutande stat fritt att välja vilken typ av ansvar för juridiska personer som ska ställas upp: straffrättsligt, civilrättsligt eller administrativt.

Det finns bestämmelser som motsvarar dem i artikel 12 i flera gemenskapsrättsliga instrument, bl.a. i en rad rambeslut som antagits inom ramen för samarbetet i rättsliga och inrikes frågor i EU. Regeringen har i flera lagstiftningsärenden som avsett genomförande av dessa rambeslut bedömt att reglerna om företagsbot i 36 kap. 7–10 a §§ brottsbalken är tillräckliga för att uppfylla kravet på sanktioner mot juridiska personer (se t.ex. propositionerna Sveriges antagande av rambeslut om åtgärder för att bekämpa sexuellt utnyttjande av barn och barnpornografi, prop. 2003/04:12 s. 38 och prop. 2006/07:66 s. 31). Detsamma gäller Europarådets konventioner om förebyggande av terrorism (ETS 196) och om bekämpande av människohandel (CETS 197) (se propositionerna Straffrättsliga åtgärder till förebyggande av terrorism, prop. 2009/10:78 s. 33–34 och Förstärkt straffrättsligt skydd mot människohandel, prop. 2009/10:152 s. 46). I det sistnämnda lagstiftningsärendet inkluderades även reglerna om förverkande i 36 kap. 4 § brottsbalken.

Det finns inte anledning att nu göra några andra överväganden. Regeringen delar därför utredningens bedömning att svensk rätt uppfyller konventionens krav på juridiska personers ansvar genom befintliga bestämmelser om företagsbot och förverkande.

Påföljder och åtgärder (artikel 13 i konventionen)

De fördragsslutande staterna ska se till att brotten i artiklarna 2–11 straffbeläggs med effektiva, proportionerliga och avskräckande påföljder, innefattande frihetsberövande för privatpersoner och ekonomiska påföljder för juridiska personer (se artikel 13). Regeringen delar utredningens bedömning att det svenska påföljdssystemet uppfyller konventionens krav på påföljder och åtgärder.

7.2 Tilläggsprotokollets krav på kriminalisering och åtgärder

Regeringens bedömning: Svensk rätt uppfyller tilläggsprotokollets krav på kriminalisering och åtgärder.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna delar eller har inget att invända mot bedömningen.

Skälen för regeringens bedömning

Rasistiskt och främlingsfientligt motiverat hot (artikel 4 i tilläggsprotokollet)

Det ska 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, om den används som svepskäl för någon av de förstnämnda utmärkande egenskaperna, eller en grupp av personer som utmärks av någon av de egenskaper som nämnts i den föregående punkten, med att begå brott som i den fördragsslutande statens nationella lagstiftning definieras som allvarliga (se artikel 4). Det är en sak för varje fördragsslutande stat att avgöra vad som är att anse som ett allvarligt brott. Hotet behöver inte ha uttryckts offentligt. Det krävs inte heller 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 och 35).

Svensk rätt bedöms främst uppfylla tilläggsprotokollets krav på kriminalisering av rasistiskt och främlingsfientligt motiverat hot genom befintliga straffbestämmelser om olaga hot (se 4 kap. 5 § brottsbalken) och hets mot folkgrupp (se 16 kap. 8 § brottsbalken). Olaga hot och hets mot folkgrupp kan, som framgått ovan, även bestraffas som tryck- och yttrandefrihetsbrott.

Medhjälp (artikel 7 i tilläggsprotokollet)

Uppsåtlig medhjälp till samtliga brott i tilläggsprotokollet ska vara straffbart (se artikel 7). I svensk rätt är anstiftan av och medhjälp till samtliga de brott som motsvarar brott enligt artiklarna 3–6 i tilläggsprotokollet straffbart (se 23 kap. 4 § brottsbalken).

Dessa brott kan i vissa fall vara att bedöma som tryck- eller yttrandefrihetsbrott. Principen om ensamansvar i tryckfrihetsförordningen och yttrandefrihetsgrundlagen innebär att vanliga straffrättsliga regler om ansvar för medverkan inte tillämpas i dessa fall. Istället åvilar straffansvaret en särskilt utpekad person. Tilläggsprotokollets ingresstext anger emellertid att artiklarna inte avser att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem. Mot den bakgrunden delar regeringen utredningens bedömning. Den svenska särregleringen kan inte anses stå i konflikt med tilläggsprotokollets krav på ansvar för medhjälp. Svensk rätt bedöms uppfylla tilläggsprotokollets krav i bestämmelsen om medhjälp genom brottsbalkens bestämmelser om medhjälp.

Juridiska personers ansvar samt påföljder och åtgärder (del av artikel 8.1 i tilläggsprotokollet)

Vissa av konventionens artiklar, däribland artikel 12 om juridiska personers ansvar och artikel 13 om påföljder och åtgärder, ska i tillämpliga delar gälla även för tilläggsprotokollet.

Regeringen anser, i likhet med utredningen, att den bedömning som gjorts under artikel 12 och 13 beträffande brotten i konventionen har motsvarande giltighet för brotten i tilläggsprotokollet. Det svenska påföljdssystemet bedöms alltså uppfylla tilläggsprotokollets krav på juridiska personers ansvar samt på påföljder och åtgärder. Det behövs inga ytterligare lagändringar för att genomföra bestämmelserna om processrätt och internationellt samarbete.

Övriga krav på kriminalisering (artikel 3,5 och 6 i tilläggsprotokollet)

De krav på kriminalisering och åtgärder som rör vissa handlingar av rasistisk och främlingsfientlig natur som finns i artiklarna 3, 5 och 6 har behandlats i avsnitt 6.4.

8 Det behövs inte några lagändringar för att genomföra övriga bestämmelser om processrätt och internationellt samarbete

8.1 De processrättsliga bestämmelserna i konventionen och tilläggsprotokollet

Regeringens bedömning: De processrättsliga bestämmelserna i konventionen om bl.a. allmänna villkor och garantier kräver i sig inga lagstiftningsåtgärder.

Svensk rätt uppfyller konventionens krav på skyldighet att lämna uppgifter.

De svenska domsrättsreglerna uppfyller konventionens och tilläggsprotokollets krav på domsrätt.

Det behövs inga andra lagändringar än de som följer av anpassningen till konventionens processrättsliga artiklar för att uppfylla de processrättsliga kraven i tilläggsprotokollet.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna delar eller har inget att invända mot bedömningen.

Skälen för regeringens bedömning

De processrättsliga bestämmelsernas räckvidd samt villkor och garantier (artikel 14 och 15 i konventionen)

Tillämpningsområdet för de processrättsliga reglerna och vilka förbehåll som får göras beträffande dessa regleras i artikel 14. Artikel 15 innehåller

bestämmelser som syftar till att garantera proportionalitet och rättssäkerheten vid införandet och användningen av tvångsmedel och andra åtgärder. Artiklarna kräver i sig inga lagstiftningsåtgärder men ska beaktas vid genomförandet av övriga processrättsliga bestämmelser.

Skyldighet att lämna uppgifter (artikel 18 i konventionen)

Det finns en allmän skyldighet för personer att lämna ut särskilt angivna datorbehandlingsbara uppgifter, och en särskild skyldighet för tjänsteleverantörer att lämna ut abonnentuppgifter (se artikel 18). Artikeln gäller enbart befintliga eller redan lagrade uppgifter.

De brottsutredande myndigheter kan få tillgång till de uppgifter som avses i artikeln från personer och teleoperatörer genom beslag (se 27 kap. 1 § rättegångsbalken), edition (se 23 kap. 14 § och 38 kap. 2 § rättegångsbalken), hemlig avlyssning eller övervakning av elektronisk kommunikation (se 27 kap. 18–19 §§) och genom bestämmelsen om utlämnande av vissa uppgifter som gäller misstanke om brott till en myndighet som ska ingripa mot brottet i 6 kap. 22 § första stycket 2 lagen om elektronisk kommunikation. Svensk rätt bedöms därmed uppfylla konventionens krav på skyldighet att lämna uppgifter.

Det kan även nämnas att Beslagsutredningens betänkande innehåller förslag som ytterligare ska öka möjligheterna att begära ut elektroniska uppgifter (se betänkandet Beslag och husrannsakan – ett regelverk för dagens behov, SOU 2017:100). Utredningens förslag har remitterats och bereds för närvarande i Regeringskansliet. Inom EU pågår också förhandlingar om införande av en europeisk bevarandeorder och en europeisk utlämnandeorder i syfte att underlätta säkrandet och insamlandet av elektroniska bevis som lagras eller innehas av tjänsteleverantörer i en annan jurisdiktion (se förslag till Europaparlamentets och rådets förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden 2018/0108 [COD]).

Domsrätt (artikel 22 i konventionen)

I artikel 22 finns bestämmelser om domsrätt. De svenska reglerna om domsrätt är vidsträckta och det finns generellt goda möjligheter att ingripa även mot brott som har begåtts utomlands (se framförallt 2 kap. brottsbalken). Regeringen delar utredningens bedömning att de svenska domsrättsreglerna uppfyller konventionens krav i denna del.

De processrättsliga bestämmelserna och reglerna om domsrätt i konventionen omfattar även tilläggsprotokollet (del av artikel 8.1 och 8.2 i tilläggsprotokollet)

De befogenheter, förfaranden och möjligheter till förbehåll som föreskrivs i konventionens processrättsliga artiklar samt reglerna om domsrätt i artikel 22 i konventionen ska även kunna tillämpas på de brott som omfattas av tilläggsprotokollet (se artikel 8.1 och 8.2).

Regeringen delar utredningens bedömning att det inte behövs några andra lagändringar än de som följer av anpassningen till konventionens processrättsliga artiklar för att uppfylla de processrättsliga kraven i tilläggsprotokollet.

8.2 Bestämmelserna om internationellt samarbete i konventionen och tilläggsprotokollet

Regeringens bedömning: Konventionens övriga bestämmelser om internationellt samarbete, bl.a. bestämmelserna om allmänna principer för internationellt samarbete, utlämning och ömsesidig rättslig hjälp samt om förfarandet, kräver inga lagstiftningsåtgärder.

Det behövs inte några andra lagändringar än de som följer av anpassningen till konventionens artiklar om internationellt samarbete för att uppfylla tilläggsprotokollets krav.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna delar eller har inget att invända mot bedömningen. *Bahnhof AB* påpekar att Sverige, oavsett vad som sägs i konventionen, borde vara så restriktivt som möjligt med vilken information om svenska medborgare och svensk brottsbekämpning som lämnas till andra länder.

Skälen för regeringens bedömning

Allmänna principer för internationellt samarbete (artikel 23 i konventionen)

Utgångspunkten för det internationella samarbetet på det område som konventionen täcker utgörs av allmänt vedertagna principer för sådant samarbete. Artikeln kräver inte några lagstiftningsåtgärder.

Principer för utlämning (artikel 24 i konventionen)

I artikel 24 regleras frågor om utlämning och lagföring vid vägrad utlämning. Bestämmelsen ställer bl.a. krav på att utlämning ska kunna ske för brott som omfattas av artiklarna 2–11 i konventionen, om brotten enligt lagstiftningen i båda staterna kan straffas med frihetsberövande och maximistraffet uppgår till lägst ett år. För utlämning gäller de villkor som anges i den anmodade statens lagstiftning eller i gällande utlämningsavtal (se artikel 24.1 och 2). Om en stat vägrar utlämning på grund av att den anser sig behörig att utreda eller lagföra brottet kan den ansökande staten kräva att utredning eller lagföring sker och resultatet återrapporteras (se artikel 24.6).

Förutsättningarna för utlämning och överlämnande finns i lagen (1957:668) om utlämning för brott, lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder och lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder. Samtliga de brott som ska vara utlämningsbara utgör som konstaterats brott enligt svensk lagstiftning och omfattas av nämnda lagar. I de fall krav på dubbel straffbarhet och en nedre gräns för maximistraffets längd uppställs överstiger det inte i något fall ett år (se 4 § lagen om utlämning för brott, 2 kap. 2 § första stycket 1 lagen om överlämnande från Sverige enligt en europeisk arresteringsorder och 2 kap. 2 § första stycket lagen om överlämnande från Sverige enligt en nordisk arresteringsorder).

Polismyndigheten eller en åklagare ska, om det finns anledning att anta att ett brott som hör under allmänt åtal har begåtts, fatta beslut om att inleda

en förundersökning (se 23 kap. rättegångsbalken). En åklagare är också skyldig att åtala brott som hör under allmänt åtal om inte något annat är särskilt föreskrivet (se 20 kap. 6 § rättegångsbalken). I ett tidigare lagstiftningsärende har regeringen ansett att dessa bestämmelser är tillräckliga för att uppfylla krav på åtgärder vid vägrad utlämning liknande det i konventionen (se propositionen Straffrättsliga åtgärder till förebyggande av terrorism, prop. 2009/10:78 s. 35–36).

Regeringen delar sammanfattningsvis utredningens bedömning att konventionens principer för utlämning inte kräver några lagstiftningsåtgärder.

Allmänna principer för ömsesidig hjälp (artikel 25 i konventionen)

I artikel 25 anges vilka allmänna principer som ska gälla för rättslig hjälp. Bestämmelserna ger, liksom artikel 23, huvudsakligen uttryck för redan etablerade allmänna principer för internationellt rättsligt samarbete. Utöver dessa allmänna principer anges också att en fördragsslutande stat i brådskande fall ska ha möjlighet att göra framställningar eller sända meddelande genom telefax eller e-post samt att rättslig hjälp inte får vägras (se artikel 25.3). Regeln är förenlig med svenska regler om möjliga kommunikationssätt (se 2 kap. 2 § förordningen om en europeisk utredningsorder och 2 kap. 4 § fjärde stycket lagen om internationell rättslig hjälp i brottmål).

Den svenska regleringen om internationell rättsligt samarbete är anpassad efter de allmänna principer som kommer till uttryck i artikeln. Regeringen bedömer, i likhet med utredningen, att bestämmelsen inte kräver några lagstiftningsåtgärder.

Upplysningar som lämnas på eget initiativ (artikel 26 i konventionen)

Inom gränsen för nationell rätt får en part på eget initiativ lämna över information till en annan part (se artikel 26).

Svenska myndigheter kan i dag frivilligt lämna information till en annan stat, med de begränsningar som gäller med hänsyn till sekretess (se t.ex. 8 kap. 3 § offentlighets- och sekretesslagen [2009:400]). De kan då ställa villkor som begränsar den mottagande statens användning av uppgifterna (se bl.a. propositionerna Europarådskonventionen om ömsesidig rättslig hjälp i brottmål – tillträde till det andra tilläggsprotokollet, prop. 2012/13:170 s. 23 och Straffrättsliga åtgärder till förebyggande av terrorism, prop. 2009/10:78 s. 37). Möjligheten att ställa villkor som begränsar den mottagande statens användning av uppgifterna finns även i annan lagstiftning (se 5 kap. 2 § lagen om internationell rättslig hjälp i brottmål).

Det finns också bestämmelser om bindande villkor för hur uppgifterna får användas när en svensk myndighet är mottagare av informationen (se 5 kap. 1 § lagen om internationell rättslig hjälp i brottmål och för polisiärt samarbete 6 kap. 3 § lagen [2017:496] om internationellt polisiärt samarbete samt 4 kap. 2 § lagen [2000:1219] om internationellt tullsamarbete).

Svensk rätt tillåter redan i dag ett sådant informationsutbyte som avses i artikel 26. Den svenska lagstiftningen om internationellt rättsligt samarbete tillhandahåller också möjligheter att ställa upp villkor för hur informationen får användas för att undvika situationer som de *Bahnhof AB* lyfter

fram. Regeringen delar därför utredningens bedömning att artikel 26 inte kräver några lagstiftningsåtgärder.

Ömsesidig rättslig hjälp när tillämpliga internationella avtal saknas (artikel 27 i konventionen)

Om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp mellan de berörda fördragsslutande staterna finns särskilda regler om detta (se artikel 27). Där regleras bland annat vilken parts lagar som styr förfarandet, vilka skäl som ska vara giltiga för ett avslag och vad som ska gälla vid en begäran om hemlighållande. Reglerna kan även tillämpas om staterna, trots att det finns ett avtal eller en överenskommelse, kommer överens om att tillämpa den. Artikeln innehåller också bestämmelser om att parterna ska utse och anmäla en centralmyndighet.

I svensk rätt finns regler om förfarandet, skäl för avslag och sekretess m.m. i ärenden om internationell rättslig hjälp i flera författningar (se lagen om internationell rättslig hjälp i brottmål, lagen om en europeisk utredningsorder, förordning om en europeisk utredningsorder och offentlighets- och sekretesslagen). Om en konventionsstat som Sverige inte har några avtal med begär att reglerna i artikel 27 ska tillämpas på en framställan om rättslig hjälp kan Sverige tillmötesgå en sådan begäran med stöd av befintlig lagstiftning och det skulle inte uppstå någon konflikt mellan regelverken. Regeringen delar utredningens bedömning att artikeln därför inte kräver några lagstiftningsåtgärder.

Sekretess och begränsningar i fråga om användning (artikel 28 i konventionen)

Det finns en möjlighet för den anmodade staten att ställa upp dels krav på sekretess, dels begränsningar i fråga om användningen (se artikel 28). Bestämmelserna är endast 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.

Som framgått finns det bestämmelser om sekretess och bindande villkor i fråga om användningen för uppgift i verksamhet som avser rättsligt samarbete både när Sverige är begärande och anmodande stat (se vad som sagts om artikel 26 ovan).

Regeringen delar utredningens bedömning att svenska myndigheter kan tillmötesgå en begäran om användningsbegränsningar från en annan fördragsslutande stat med stöd av dessa bestämmelser och det anses därför inte krävas några lagstiftningsåtgärder för att uppfylla kraven i artikel 28.

Ömsesidig rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter (artikel 31 i konventionen)

Artikel 31 innehåller bestämmelser om rättslig hjälp med åtkomst till lagrade och säkrade datorbehandlingsbara uppgifter. Det är sådana åtgärder som omfattas av artikel 19 som avses (se den förklarande rapporten p. 292). 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 enligt kapitel III i konventionen (huvudsakligen artikel 25 och 27).

Regeringen gör bedömningen att svensk rätt uppfyller kraven i artikel 19.1–3 genom bestämmelserna om husrannsakan och beslag i 27 och 28 kap. rättegångsbalken. Rättslig hjälp med husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter omfattas av lagen om internationell rättslig hjälp i brottmål och en utredningsorder kan avse dessa åtgärder (se 1 kap. 2 § lagen om internationell rättslig hjälp i brottmål och 1 kap. 4 § lagen om en europeisk utredningsorder).

Regeringen delar utredningens bedömning att svensk rätt uppfyller kraven i artikel 31 och att det inte krävs några ytterligare lagstiftningsåtgärder.

Gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter med samtycke eller i de fall de är allmänt tillgängliga (artikel 32 i konventionen)

En fördragsslutande stat får utan tillstånd av en annan sådan stat bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter i vissa fall (se artikel 32). Bestämmelsen är i det närmaste 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 situationer som avses är sådana som alla parter var eniga om redan är folkrättsligt tillåtna (se den förklarande rapporten p. 293).

Regeringen delar utredningens bedömning att artikeln inte kräver några lagstiftningsåtgärder.

Ömsesidig rättslig hjälp med insamling i realtid av trafikuppgifter (artikel 33 i konventionen) och med avlyssning av innehållsuppgifter (artikel 34 i konventionen)

Artikel 33 innehåller bestämmelser om rättslig hjälp med insamling av trafikuppgifter i realtid. För denna hjälp ska gälla de villkor och förfaranden som anges i den nationella lagstiftningen. Staterna ska emellertid lämna sådan hjälp åtminstone med avseende på brott för vilka insamling i realtid av trafikuppgifter skulle vara möjlig i ett motsvarande nationellt fall.

De fördragsslutande staterna 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, se artikel 34. 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.

Regeringen har ovan gjort bedömningen att svensk rätt genom bestämmelserna om hemlig övervakning och avlyssning av elektronisk kommunikation uppfyller konventionens krav på insamling av trafik- och innehållsuppgifter i realtid enligt artikel 20 och 21, om ett visst förbehåll lämnas. Rättslig hjälp med såväl hemlig övervakning som hemlig avlyssning av elektronisk kommunikation kan lämnas med stöd av lagen om internationell rättslig hjälp i brottmål och en utredningsorder kan avse dessa åtgärder (se 1 kap. 2 § lagen om internationell rättslig hjälp i brottmål och 1 kap.

4 § lagen om en europeisk utredningsorder). Rättslig hjälp lämnas huvudsakligen under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning (se 2 kap. 1 § första stycket lagen om internationell rättslig hjälp i brottmål och 3 kap. 4 § lagen om en europeisk utredningsorder).

Sammanfattningsvis bedöms svensk rätt uppfylla kraven i artikel 33 och 34 om ett sådant förbehåll enligt artiklarna 20 och 21 som föreslagits ovan lämnas. Några lagstiftningsåtgärder krävs inte.

Nätverk (artikel 35 i konventionen)

Varje fördragsslutande stat ska utse en kontaktpunkt med tillgång till utbildad personal och utrustning (se artikel 35). Kontaktpunkten 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.

Regeringen delar utredningens bedömning att artikel 35 inte kräver några lagstiftningsåtgärder. Regeringen avser att i förordning återkomma med en närmare reglering av den svenska kontaktpunktens placering.

Bestämmelser om internationellt samarbete i tilläggsprotokollet (del av artikel 8.2 i tilläggsprotokollet)

Konventionens bestämmelser om internationellt rättsligt samarbete ska även kunna tillämpas på de brott som omfattas av tilläggsprotokollet (se artikel 8.2).

De analyser som gjorts i avsnitten 6 och 8 med utgångspunkt i konventionens bestämmelser om internationellt samarbete äger motsvarande tillämpning i förhållande till brotten i tilläggsprotokollet. De svenska bestämmelser om rättslig hjälp som beskrivs där, kan tillämpas även i förhållande till de brott som upptas i tilläggsprotokollet. I den utsträckning konventionens kräver lagändringar är detta av relevans även för tilläggsprotokollet. Regeringen delar alltså utredningens bedömning att det inte behövs några andra lagändringar än de som följer av anpassningen till konventionens artiklar om internationellt samarbete för att uppfylla tilläggsprotokollets krav.

9 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: De föreslagna ändringarna ska träda i kraft den 1 maj 2021.

Regeringens bedömning: Det finns inte något behov av övergångsbestämmelser.

Utredningens förslag och bedömning överensstämmer i huvudsak med regeringens. Utredningen föreslår en annan tidpunkt för ikraftträdandet.

Remissinstanserna: En majoritet av remissinstanserna delar eller har inget att invända mot förslaget och bedömningen. *Ekobrottsmyndigheten* önskar ett tidigare ikraftträdande än som föreslagits av utredningen.

Skälen för regeringens förslag och bedömning: De lagändringar som har föreslagits bör träda i kraft så snart som möjligt för att möjliggöra ett svenskt tillträde till Budapestkonventionen och tilläggsprotokollet. Regeringen bedömer att så kan ske tidigast den 1 maj 2021.

Utgångspunkten är att ny processrättslig lagstiftning ska tillämpas genast efter ikraftträdandet. Några övergångsbestämmelser behövs därför inte.

10 Konsekvenser av förslagen

Regeringens bedömning: De marginella kostnadsökningarna för rättsväsendet och Post- och telestyrelsen kan hanteras inom beräknade anslag.

Förslagen kan antas medföra positiva effekter för det brottsförebyggande och brottsbekämpande arbetet.

Förslagen kan komma att medföra vissa kostnader för företag som får ett föreläggande om bevarande riktat mot sig. Kostnaderna bedöms generellt bli små.

Förslagen förväntas inte få betydelse för miljön eller för jämställdheten mellan kvinnor och män.

Utredningens bedömning överensstämmer huvudsakligen med regeringens.

Remissinstanserna: En majoritet av remissinstanserna delar eller har inget att invända mot bedömningen. *Domstolsverket* anser att bedömningen om kostnadskonsekvenser är rimlig men vill påpeka att även om antalet mål inte kan förväntas öka i någon större utsträckning så kan ett flertal mindre resurskrävande reformer av nu aktuellt slag sammantaget medföra att ett resurstillskott till Sveriges Domstolar är nödvändigt. *Göteborgs tingsrätt* påpekar att införandet av ytterligare straffprocessuella tvångsmedel kan komma att öka arbetsbelastningen för såväl domstolarna som Åklagarmyndigheten. *Migrationsverket* anser att det kan uppstå kostnader vid föreläggande om bevarande av lagrade uppgifter. *Rättighetsalliansen* påpekar att kostnaderna för den som åläggs att bevara information tenderar att överskattas. En alltför frikostig ersättningsmodell innebär i praktiken en inkomstkälla för exempelvis ett företag med många kunder som är misstänkta för kriminalitet. Därför förordas en restriktiv ersättningsmodell.

Skälen för regeringens bedömning

Konsekvenser för staten

Regeringen lämnar förslag till ett nytt straffprocessuellt tvångsmedel, föreläggande att bevara en viss lagrad uppgift. Det är svårt att med någon säkerhet uppskatta hur många beslut om föreläggande om bevarande som kommer att fattas. Förslaget förväntas bidra till en mer effektiv

bekämpning av såväl brottslighet som är direkt it-relaterad som annan brottslighet där det finns bevisning i elektronisk form. Detta innebär i sin tur att fler brottsutredningar sannolikt kommer att leda till åtal och lagföring. Även om det är svårt att bedöma hur många mål det kommer att röra sig om årligen bör det med en grov uppskattning inte vara fråga om mer än ett femtiotal.

Att fler brottsutredningar leder till åtal innebär, som *Domstolsverket*, *Göteborgs tingsrätt* och *Migrationsverket* påpekar, i viss mån ökade kostnader för framförallt polis-, åklagar- och domstolsväsendet. Den förväntat ökade lagföringen kan leda till fler fängelse- eller frivårdspåföljder vilket kan leda till ökade kostnader för Kriminalvården. De kostnader som förväntas uppkomma för rättsväsendet bedöms emellertid, med hänsyn till det begränsade antal mål det kan bli fråga om, bli små och rymmas inom beräknade anslag.

Ett föreläggande om att bevara vissa lagrade uppgifter kan underställas rättens prövning. Möjligheten förväntas utnyttjas i ett fåtal fall. Kostnaderna för domstolarna och Åklagarmyndigheten hänförliga till möjligheten att överklaga bedöms därför bli mycket begränsade.

Den nya regleringen förväntas också innebära effektivitetsvinster för polis-, åklagar- och domstolsväsendet eftersom föreläggande om bevarande bedöms kunna ersätta andra, mer resurskrävande tvångsmedel i viss utsträckning. De kostnadsbesparingar som förslaget innebär bedöms emellertid bli begränsade.

De tillkommande arbetsuppgifter konventionsåtagandet innebär för den myndighet som genom bestämmelser i förordning ges funktionen att vara kontaktpunkt enligt artikel 35 förväntas inte ge upphov till annat än begränsade kostnader.

Sammanfattningsvis delar regeringen utredningens bedömning att ett konventionstillträde inte kommer att leda till mer än begränsade kostnadsökningar för rättsväsendet. Dessa ökningar bör kunna finansieras inom ramen för beräknade anslag.

Den myndighet som utöver rättsväsendet kan komma att påverkas av regeringens förslag är Post- och telestyrelsen. Post- och telestyrelsens tillsynsansvar och ansvar för att meddela föreskrifter om ersättning kommer även att omfatta de föreslagna bestämmelserna i lagen om elektronisk kommunikation. Regeringen bedömer, i likhet med utredningen, att denna utvidgning av ansvaret är mycket begränsad. De tillkommande arbetsuppgifter konventionsåtagandet innebär blir inte mer resurskrävande än att det ryms inom Post- och telestyrelsens beräknade anslag.

Konsekvenser för brottsligheten och det brottsförebyggande arbetet

De förslag som lämnas kommer att göra det möjligt för Sverige att tillträda Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll. Ett tillträde till konventionen och tilläggsprotokollet kommer att underlätta Sveriges möjligheter att få hjälp och hjälpa andra stater antingen genom rättslig hjälp eller en europeisk utredningsorder på området för it-relaterad brottslighet och att aktivt delta i det internationella brottsförebyggande och brottsbekämpande arbetet. Förslagen kan därför antas medföra positiva effekter för det brottsförebyggande och brottsbekämpande arbetet både nationellt och internationellt. Förslagen kan också förväntas bidra till

det jämställdhetspolitiska delmålet om att mäns våld mot kvinnor ska upphöra.

Konsekvenser för företag

Ett föreläggande om bevarande ska kunna riktas mot såväl fysiska som juridiska personer och mot leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Det är svårt att med någon säkerhet uppskatta hur många beslut om förelägganden som kommer att fattas men det kommer med stor sannolikhet inte att vara särskilt många per år.

Föreläggandet ska avse en viss lagrad uppgift, vilket innebär dels att uppgiften redan måste finnas lagrad hos den som föreläggandet riktar sig mot, dels att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras. Föreläggandet kan varken innebära att uppgifter som inte är lagrade ska bevaras eller 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 annat alternativ är att uppgiften lämnas orubbad på sin ursprungliga plats, samtidigt som åtgärder vidtas så att den inte kan raderas eller ändras på något sätt. Dessa åtgärder kan inte förväntas medföra mer än begränsade kostnader för ett företag.

Mot den bakgrunden kan förslagen få en högst marginell påverkan på berörda företags kostnader. Detsamma gäller den skyldighet att lämna ut uppgifter om vilka övriga leverantörer som har deltagit vid överföringen som föreslås. Uppgifter om vilka övriga leverantörer som deltagit vid överföringen av ett meddelande borde i den övervägande delen av fallen kunna fås fram genom de trafikuppgifter som lagras enligt 6 kap. 16 a § lagen om elektronisk kommunikation. Leverantörerna kommer då, enligt 6 kap. 16 e § samma lag, ha rätt till ersättning för kostnader som uppstår i samband med att uppgiften lämnas ut.

Konsekvenser i övrigt

Förslagen förväntas inte få betydelse för miljön.

11 Författningskommentar

11.1 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 det anges hur länge uppgiften ska bevaras. Tiden får inte bestämmas till längre än nödvändigt och får inte överstiga 90 dagar från dagen för beslutet.

Om det finns särskilda skäl får tiden för bevarande förlängas med högst 90 dagar.

Ett föreläggande får inte riktas mot den som skäligen kan misstänkas för brottet eller mot någon till honom eller henne sådan närstående person som avses i 36 kap. 3 §.

Paragrafen, som är ny, innehåller bestämmelser som gör det möjligt för brottsutredande myndigheter att skyndsamt säkra och bevara lagrade elektroniska uppgifter som kan antas ha betydelse för utredningen om ett brott. Övervägandena finns i avsnitt 6.1.1.

Av *första stycket* framgår 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 uppgifter som avses kan vara av vilket slag som helst, t.ex. en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat. Att uppgiften ska vara lagrad betyder att den ska finnas bevarad elektroniskt. Både sådana uppgifter som finns lagrade på grund av regler om datalagring och sådana som lagrats av annan anledning omfattas alltså. Uppgifter som har lagrats av annan anledning kan t.ex. vara uppgifter som hos tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster behandlats för fakturahantering eller liknande. Uppgiften måste finnas lagrad när föreläggandet meddelas. Det går inte att med stöd av paragrafen förelägga någon att lagra eller spara eventuella framtida uppgifter.

Att föreläggandet ska avse en viss elektronisk uppgift innebär att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan alltså inte vara generellt och t.ex. utan närmare specificering endast ange att alla uppgifter som mottagits under en tid ska bevaras.

Ett föreläggande kan rikta sig mot vem som helst som innehar en lagrad uppgift. Både fysiska och juridiska personer omfattas av bestämmelsen. Föreläggandet kan även avse lagrade uppgifter som innehas av flera olika personer samtidigt, t.ex. någons e-post som han eller hon har lagrad på en server hos en annan person. Ett föreläggande kan då riktas såväl mot den person hos vilken uppgifterna finns lagrade (den som innehar servern) som den person som på distans har kontroll över och åtkomst till uppgifterna (den person som innehar e-postkontot).

Det finns flera möjliga sätt att efterkomma ett föreläggande, t.ex. genom kopiering av uppgiften eller genom att vidta åtgärder för att uppgiften lämnas orubbad på sin ursprungliga plats. Vid behov får den som har beslutat om föreläggandet ge anvisningar om hur uppgiften ska bevaras i det enskilda fallet. Sådana anvisningar kan ges i samråd med den som föreläggandet riktar sig mot.

Att uppgiften skäligen kan antas ha betydelse för utredningen om ett brott innebär ett relativt lågt ställt krav på uppgiftens betydelse ur bevissynpunkt och innebär att åtgärden kan vidtas i ett tidigt skede av en brottsutredning. Det behöver inte finnas någon som är misstänkt för brottet.

Av *andra stycket* framgår att det i föreläggandet ska anges hur länge 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 som huvudregel inte får överstiga 90 dagar från dagen för beslutet.

Bestämmelsen i *tredje stycket* innebär att tiden för bevarande får förlängas med upp till 90 dagar om det finns särskilda skäl. Särskilda skäl kan

t.ex. vara att utredande myndighet måste vänta in uppgifter från eller åtgärder i utlandet för att kunna besluta om de bevarande uppgifterna ska begäras ut. Det kan också handla om mer komplicerade utredningar där en stor del av informationen är krypterad eller skyddas på annat sätt. Även i dessa fall kan det ta tid att ta ställning till om de bevarade uppgifterna behövs. Inte heller vid förlängning ska tiden bestämmas till längre än nödvändigt. Tiden kan förlängas vid ett eller flera tillfällen så länge den maximala tiden för förlängning om 90 dagar inte överskrids.

Fjärde stycket innehåller ett förbud mot att rikta ett föreläggande mot den som skäligen kan misstänkas för det brott som utreds. Ett föreläggande får i de fallen inte heller riktas mot någon som är närstående till den misstänkte på ett sådant sätt som avses i 36 kap. 3 § rättegångsbalken.

16 a § *Ett föreläggande enligt 16 § får beslutas av undersökningsledaren eller en åklagare.*

I föreläggandet får det anges att den som har förelagts att bevara en viss uppgift inte får uppenbara att åtgärden har vidtagits.

Den som har förelagts att bevara en viss uppgift får begära rättens prövning av föreläggandet. För rättens prövning gäller 6 § första stycket.

Paragrafen, som är ny, innehåller bestämmelser om förfarandet och om tystnadsplikt vid förelägganden att bevara en viss lagrad uppgift. Övervägandena finns i avsnitt 6.1.1.

I *första stycket* anges att undersökningsledaren eller en åklagare får utfärda ett föreläggande enligt 16 §. Under vissa förutsättningar kommer även Tullverket med stöd av 19 § lagen (2000:1225) om straff för smuggling och Kustbevakningen med stöd av 3 kap. 3 § kustbevakningslagen (2019:32) kunna besluta om ett föreläggande. Ett föreläggande om bevarande ska som utgångspunkt vara skriftligt. Föreläggandets omfattning ska tydligt framgå av beslutet. Om det i brådskande fall inte är möjligt att ge ett skriftligt föreläggande finns det inte något hinder mot att föreläggandet ges muntligen och att den som har förelagts därefter informeras skriftligen om beslutet, t.ex. om ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande.

Av *andra stycket* följer att undersökningsledaren eller åklagaren får besluta att den som har förelagts att bevara en viss uppgift inte får uppenbara att åtgärden har vidtagits. Ett sådant beslut ska framgå av föreläggandet.

Enligt *tredje stycket* får den förelagde begära rättens prövning av föreläggandet. För rättens prövning gäller samma regler som för prövning av beslag enligt 27 kap. 6 § första stycket rättegångsbalken. 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 till domstolen. Föreläggandet gäller fram till dess att rätten eller den som har utfärdat föreläggandet meddelar något annat. Frågan om ett föreläggande ska bestå är en sak mellan den som förelagts och den som meddelat föreläggandet.

Frågan om ett bevarandet ska bestå under den tid som anges i föreläggandet ska avgöras med utgångspunkt i förhållandena vid rättens prövning. I samband med att rätten prövar frågan om ett föreläggande om bevarande ska den även ta ställning till frågan om sekretess för de uppgifter

ett beslut om tystnadsplikt avser (se 18 kap. 1 § och 43 kap. 8 § offentlighets- och sekretesslagen [2009:400]).

11.2 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 att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,
7. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
8. hemlig kameraövervakning,
9. hemlig rumsavlyssning,
10. hemlig dataavläsning,
11. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,
12. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,
13. överförande av frihetsberövade för förhör m.m., och
14. rättsmedicinsk undersökning av en avliden person.

Lagen hindrar inte att hjälp lämnas med någon 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 de åtgärder som omfattas av rättslig hjälp enligt lagen. Övervägandena finns i avsnitt 6.1.2.

En ny *sjätte punkt* införs som innebär att rättslig hjälp enligt lagen kan ges med ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken. I övrigt ändras paragrafen redaktionellt på så sätt att punkterna delvis numreras om i anledning av den nya punkten 6.

2 kap.

1 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–*10* och *14* 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 *11–13* 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 paragrafen regleras vilka förutsättningar som ska gälla för tillämpning av de olika formerna av rättslig hjälp som avses i 1 kap. 2 §. Övervägandena finns i avsnitt 6.1.2.

Ändringen i *första stycket* innebär att rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken 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.

Eftersom rättslig hjälp enligt 2 kap. 1 § ska lämnas under samma förutsättningar som en motsvarande åtgärd under en svensk förundersökning får förordnandet inte gälla längre än den tid som anges i 27 kap. 16 § andra och tredje styckena rättegångsbalken, dvs. inte längre än nödvändigt och som utgångspunkt inte överstiga 90 dagar med en möjlighet till förlängning med högst 90 dagar om det finns särskilda skäl.

Övriga ändringar är redaktionella och är en följd av att punkterna i 1 kap. 2 § delvis numreras om.

2 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *6, 11* och *13* 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*, 7–10*, *12* och *14* 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.

I paragrafen regleras när dubbel straffbarhet uppställs som krav för att rättslig hjälp ska få lämnas. Övervägandena finns i avsnitt 6.1.2.

Ändringen innebär att rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift får lämnas utan något krav på dubbel straffbarhet. Övriga ändringar är redaktionella och är en följd av att punkterna i 1 kap. 2 § delvis numreras om.

4 kap.

Föreläggande att bevara en viss lagrad uppgift

24 c § *En ansökan om ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken handläggs av en åklagare.*

I paragrafen, som är ny, regleras vem som handlägger en ansökan om rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift. Övervägandena finns i avsnitt 6.1.2.

Av paragrafen följer att en ansökan om rättslig hjälp med ett föreläggande handläggs av en åklagare.

11.3 Förslaget till lag om ändring i lagen (2003:389) om elektronisk kommunikation

6 kap.

8 § Bestämmelserna i 5–7 §§ gäller inte

1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 5 § för att lösa tvister,

2. för elektroniska meddelanden som omfattas av ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,

3. för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, eller

4. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Paragrafen reglerar undantag från tillhandahållarnas skyldighet att utplåna och avidentifiera trafikuppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande. Övervägandena finns i avsnitt 6.1.1.

En ny *andra punkt* införs som innebär att undantaget har utvidgats till att även omfatta uppgifter som har begärts bevarade enligt 27 kap. 16 § rättegångsbalken.

I övrigt ändras paragrafen redaktionellt på så sätt att punkterna delvis numreras om i anledning av den nya punkten 2.

16 c § Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 *eller 14*, 27 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Paragrafen anger när uppgifter som har lagrats enligt 6 kap. 16 a § får behandlas. Övervägandena finns i avsnitt 6.2.1.

Ändringen innebär att uppgifter som har lagrats enligt 6 kap. 16 a § även får behandlas för att lämnas ut enligt 6 kap. 22 § första stycket 14. Se vidare kommentaren till 6 kap. 22 §.

16 d § Uppgifter som avses i 16 a § ska lagras enligt följande:

– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock lagras i endast två månader.

– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de dock lagras i endast sex månader.

Lagringstiden räknas från den dag kommunikationen avslutades.

När lagringstiden *har* löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande har kommit in *eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har meddelats* innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de *har* lämnats ut *eller tiden för bevarande har löpt ut*. *Därefter* ska uppgifterna genast utplånas.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om lagringstiden enligt första stycket.

Paragrafen anger lagringstidens längd och de åtgärder som ska vidtas från den lagringsskyldiges sida vid lagringstidens slut. Övervägandena finns i avsnitt 6.1.1.

Ändringen i *tredje stycket* innebär att uppgifter som ska bevaras enligt 27 kap. 16 § rättegångsbalken inte ska utplånas innan tiden för bevarandet har löpt ut.

16 g § *Om någon som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § har förelagts att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken gäller 3 a, 16 e och 16 f §§ på motsvarande sätt för den uppgift som ska bevaras.*

Paragrafen, som är ny, innebär att bestämmelserna i 6 kap. 3 a, 16 e och 16 f §§ även ska gälla när en uppgift bevaras på grund av ett föreläggande enligt 27 kap. 16 § rättegångsbalken. Övervägandena finns i avsnitt 6.1.1.

Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § och bevarar uppgifter på grund av ett föreläggande enligt 27 kap. 16 § rättegångsbalken ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de bevarade uppgifterna vid behandling. Regeringen eller den myndighet som regeringen bestämmer får meddela närmare föreskrifter om sådana skyddsåtgärder (jfr 3 a §).

Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § och bevarar uppgifter på grund av ett föreläggande enligt 27 kap. 16 § rättegångsbalken har också rätt till ersättning för kostnader som uppstår när bevarade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna. Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om ersättningen (jfr 16 e §).

Vidare ska den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § och bevarar uppgifter på grund av ett föreläggande enligt 27 kap. 16 § rättegångsbalken bedriva verksamheten så att uppgifterna utan dröjsmål kan lämnas ut och så att verkställighet av utlämnandet inte röjs. Uppgifterna ska göras tillgängliga på ett sådant sätt att informationen enkelt kan tas omhand (jfr 16 f §).

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 en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken, och

7. begäran om utlämnande av en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster enligt 22 § första stycket 14.

Paragrafen innehåller regler om tystnadsplikt för tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Övervägandena finns i avsnitt 6.1.1. och 6.2.1.

Två nya punkter införs i bestämmelsen, *punkterna 6* och *7*. Ändringen innebär att tystnadsplikt enligt 20 § första stycket ska gälla för uppgift som hänför sig till ett föreläggande om bevarande enligt 27 kap. 16 § rättegångsbalken. Tystnadsplikt ska också gälla för uppgift som hänför sig till en begäran från en myndighet att få tillgång till uppgifter om vilka andra tillhandahållare som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande om bevarande enligt 6 kap. 22 § första stycket 14 i lagen. Övriga ändringar är redaktionella.

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 en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen 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 Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns 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 Polismyndigheten, 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 Polismyndigheten eller en 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,

9. uppgift som avses i 20 § första stycket 1 till Finansinspektionen, om inspektionen finner att uppgiften är av väsentlig betydelse för utredningen av en misstänkt

överträdelse av Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentet och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG,

10. uppgift som avses i 20 § första stycket 1 till Finansinspektionen, om inspektionen finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller någon av bestämmelserna i 4 a kap. 1–8 §§ lagen (2010:751) om betaltjänster eller 1 kap. 5 § eller 4 kap. 7, 8, 9, 10, 11 eller 14 § lagen (2016:1024) om verksamhet med bostadskrediter,

11. uppgift som avses i 20 § första stycket 1 till Konsumentombudsmannen, om ombudsmannen finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden eller marknadsföringslagen (2008:486), när det är fråga om en misstänkt överträdelse av unionslagstiftning som skyddar konsumenternas intressen enligt bilagan till Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004,

12. uppgift som avses i 20 § första stycket 1 till Läkemedelsverket, om verket finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i 12 kap. läkemedelslagen (2015:315), och

13. uppgift som avses i 20 § första stycket 1 till Konsumentverket, om verket finner att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning*, och*

14. uppgift som avses i 20 § första stycket 3 om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § 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 tillhandahållares skyldighet att på begäran lämna ut vissa uppgifter som enligt huvudregeln i 6 kap. 20 § första stycket omfattas av tystnadsplikt. Övervägandena finns i avsnitt 6.2.1.

En ny punkt införs i paragrafen, *punkt 14*. Den nya bestämmelsen innebär att den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till en uppgift som avses i 6 kap. 20 § första stycket 3 ska vara skyldig att till den myndighet som beslutat om ett föreläggande enligt 27 kap. 16 § rättegångsbalken lämna ut en uppgift om vilka övriga tillhandahållare 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 tillhandahållare som deltagit vid överföringen så att ett föreläggande kan riktas även mot dessa. En förutsättning för uppgiftsskyldigheten är att tillhandahållaren har förelagts att bevara en viss uppgift enligt 27 kap. 16 § rättegångsbalken. Uppgiftsskyldigheten är också begränsad till just information om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av det meddelande som omfattas av föreläggandet.

Den myndighet som har beslutat om föreläggandet har alltså endast möjlighet att få reda på från vilken tillhandahållare som meddelandet sändes och, för det fall det har sänts vidare, till vilken tillhandahållare det sändes. Det ankommer på tillhandahållaren att ur den information som avses i 6 kap. 20 § första stycket 3 ta reda på vilka dessa tillhandahållare är. Om trafikuppgifterna inte innehåller informationen kan tillhandahållaren förstås inte heller lämna ut den. Övriga ändringar är redaktionella.

11.4 Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

1 kap.

4 § En utredningsåtgärd enligt denna lag ska avse eller motsvara
1. förhör under förundersökning,
2. bevisupptagning vid domstol,
3. förhör genom ljudöverföring eller ljud- och bildöverföring,
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § *eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 §* samma balk,
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,
7. tillfälligt överförande av en frihetsberövad person,
8. rättsmedicinsk undersökning av en avliden person,
9. kontrollerad leverans,
10. bistånd i en brottsutredning med användning av en skyddsidentitet,
11. inhämtande av bevis som finns hos en myndighet, eller
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.

I paragrafen finns en uttömmande uppräkning av de utredningsåtgärder som ska avse eller motsvara en utredningsorder. Övervägandena finns i avsnitt 6.1.3.

Ändringen i *första stycket 4* innebär att Sverige ska kunna utfärda eller erkänna och verkställa en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken.

Förslaget att föra in ett föreläggande om bevarande som en ny åtgärd i fjärde punkten innebär att en åklagare kommer att kunna utfärda en utredningsorder för ett sådant föreläggande, vilket framgår av 2 kap. 1 §. Det innebär också att erkännande och verkställighet får vägras om förutsättningarna för det i 3 kap. 7 § är uppfyllda.

2 kap.

Föreläggande att bevara en viss lagrad uppgift

16 a § *När en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har verkställts i den andra medlemsstaten får den som har förelagts åtgärden begära rättens prövning. För rättens prövning gäller 27 kap. 6 § första stycket samma balk.*

Den tid en uppgift enligt 27 kap. 16 § andra stycket rättegångsbalken ska bevaras, räknas från den tidpunkt då åtgärden verkställdes i den andra medlemsstaten. Om det finns särskilda skäl får tiden för bevarande förlängas med högst 90 dagar.

Paragrafen, som är ny, anger vad som särskilt ska gälla när en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift har utfärdats. Övervägandena finns i avsnitt 6.1.3.

Av *första stycket* följer att när en utredningsorder för ett föreläggande enligt 27 kap. 16 § rättegångsbalken har verkställts i den andra medlemsstaten får den som har förelagts åtgärden begära prövning av beslutet i domstol. För rättens prövning ska samma regler gälla som vid prövningen av ett föreläggande i en nationell situation, det vill säga vad som enligt 27 kap. 6 § första stycket rättegångsbalken gäller för beslag. Rätten ska 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 till domstolen.

Av bestämmelsen i *andra stycket första meningen* följer att tiden för bevarande ska räknas från verkställighetstidpunkten i den andra medlemsstaten. Den ordningen beror av att en utredningsorder för ett föreläggande om bevarande behöver kunna bestå under den tid som den andra medlemsstaten har på sig för att erkänna och verkställa dels utredningsordern för att bevara lagrade uppgifter, dels en efterföljande utredningsorder för röjande av uppgifterna. Den andra medlemsstatens behöriga myndigheter har i regel 30 dagar på sig för att fatta beslut om att erkänna och verkställa en utredningsorder och därefter 90 dagar för att genomföra utredningsåtgärden (se artikel 12 Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området).

Av bestämmelsen i *andra stycket andra meningen* framgår att samma möjligheter till förlängning av tiden för bevarande finns som i en nationell situation. Att det krävs särskilda skäl innebär att möjligheten till förlängning enbart ska utnyttjas när det på grund av någon särskild omständighet är nödvändigt för att de bevarade uppgifterna inte ska utplånas innan en utredningsorder för en åtgärd om röjande har hunnit verkställas. Se vidare kommentaren till 27 kap. 16 § rättegångsbalken. Inte heller vid en förlängning ska tiden bestämmas till längre än nödvändigt. Tiden för bevarande kan förlängas vid ett eller flera tillfällen så länge fristerna inte överskrids.

3 kap.

5 § En utredningsorder får inte erkännas och verkställas i Sverige om

1. det skulle strida mot bestämmelser om immunitet och privilegier eller om skydd för uppgifter som avses i 36 kap. 5 och 5 a §§ rättegångsbalken,

2. ordern avser beslag av en skriftlig handling eller ett skriftligt meddelande *eller ett föreläggande att bevara en viss lagrad uppgift* och det enligt 27 kap. 2 § rättegångsbalken finns hinder mot att ta handlingen eller meddelandet i beslag *eller enligt 27 kap. 16 § fjärde stycket samma balk meddela ett föreläggande*,

3. det skulle medföra fara för Sveriges säkerhet, äventyra enskilda personers säkerhet eller medföra risk för röjande av uppgifter som rör underrättelseverksamhet,

4. den gärning som avses i utredningsordern har begåtts utanför den utfärdande medlemsstatens territorium och helt eller delvis i Sverige, och gärningen inte motsvarar ett brott enligt svensk lag, eller

5. utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 §.

En utredningsorder får inte vägras enligt första stycket 5, om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser.

I paragrafen finns bestämmelser om när en utredningsorder inte får erkännas och verkställas i Sverige. Övervägandena finns i avsnitt 6.1.3.

Ändringen i *första stycket 2* innebär att en utredningsorder för ett föreläggande om bevarande inte får erkännas och verkställas om den som föreläggandet riktar sig mot skäligen kan misstänkas för det brott som utreds. Detsamma gäller om den som föreläggandet riktar sig mot är närstående till den misstänkte på ett sådant sätt som avses i 36 kap. 3 § rättegångsbalken.

Föreläggande att bevara en viss lagrad uppgift

33 a § *När en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har verkställts, tillämpas 32 § första, fjärde och femte styckena.*

Paragrafen, som är ny, anger vilka bestämmelser som särskilt ska gälla vid verkställighet av en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift. Övervägandena finns i avsnitt 6.1.3.

Av pargrafen framgår att när en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift har verkställts i Sverige får den som åtgärden har riktats mot begära prövning av verkställbarhetsförklaringen i domstol. Behörig domstol är den tingsrätt inom vars domkrets föreläggandet har verkställts. Om domstolen vid sin prövning finner att verkställbarhetsförklaringen ska upphävas, ska de verkställighetsåtgärder som har vidtagits återgå, så långt det är möjligt (jfr 32 §). Det innebär att föreläggandet inte längre gäller och att de lagrade uppgifterna inte behöver bevaras.

Att tiden för bevarande räknas från beslutet om verkställighet följer av 27 kap. 16 § rättegångsbalken.

4 kap.

1 § Domstolens beslut enligt 2 kap. 5, 14, 16 *och 16 a* §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *om* den åtgärd som avses i utredningsordern.

Ett beslut i fråga om att utfärda en utredningsorder får inte överklagas.

I paragrafen finns bestämmelser om överklagande av domstolens beslut i vissa fall. Övervägandena finns i avsnitt 6.1.3.

Ändringen i *första stycket* innebär att domstolens beslut i fråga om utfärdande av en utredningsorder för ett föreläggande om bevarande enligt 2 kap. 16 a § får överklagas. Vidare görs en ändring av språklig karaktär.

2 § Domstolens beslut enligt 3 kap. 9, 32*,* 33 *och 33 a* §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *om* en åtgärd som motsvarar den åtgärd som avses i utredningsordern. Domstolens beslut enligt 3 kap. 25 § får överklagas på det sätt som gäller enligt rättegångsbalken.

Övriga beslut i fråga om erkännande och verkställighet av en utredningsorder får inte överklagas.

I paragrafen finns bestämmelser om överklagande av domstolens beslut i vissa fall. Övervägandena finns i avsnitt 6.1.3.

Ändringen i *första stycket* innebär att domstolens beslut om verkställighetsförklaring för en utredningsorder för ett föreläggande om bevarande enligt 3 kap. 33 a § får överklagas. Vidare görs en ändring av språklig karaktär.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

European Treaty Series - No. 185

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Europarådets konvention om it-relaterad brottslighet (ETS 185) och tillägsprotokollet (ETS 189)

Europarådets konvention om it-relaterad brottslighet (ETS 185)

(Inofficiell översättning)

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 föreläggande 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 omöjliggör verkställandet av framställningen eller sannolikt kan försena det avsevärt.

8. Den begärande parten får anhålla om att den anmodade parten hemlighåller att en framställning har gjorts med stöd av detta kapitel liksom dess syfte, utom i den mån det är nödvändigt för dess verkställande att röja uppgiften. Om den anmodade parten inte kan tillmötesgå anhållan om hemlighållande, ska den oförd röjligen 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 överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av uppgifterna.

2. En framställning om säkrande som görs med stöd av punkt 1 i denna artikel 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 generalsekreteraren 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.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

European Treaty Series - No. 189

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Strasbourg, 28.I.2003

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as "the Convention"), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1 For the purposes of this Protocol:

"*racist and xenophobic material*" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2 A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2 A Party may either:

a require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1 Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2 A Party may either

a require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

1 Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol.

2 The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Chapter IV – Final provisions

Article 9 – Expression of consent to be bound

1 This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

a signature without reservation as to ratification, acceptance or approval; or

b subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3 The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1 This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2 In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11 – Accession

1 After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2 Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12 – Reservations and declarations

1 Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.

2 By a written notification addressed to the Secretary General of the Council of Europe, any Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3 By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

Article 13 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14 – Territorial application

1 Any Party may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Protocol shall apply.

2 Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 15 – Denunciation

1 Any Party may, at any time, denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 16 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Protocol in accordance with its Articles 9, 10 and 11;

d any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 28th day of January 2003, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Protocol, and to any State invited to accede to it.

Tilläggsprotokoll till konventionen om it-relaterad brottslighet om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem (ETS 189)

(Inofficiell översättning)

Strasbourg den 28 januari 2003

Medlemsstaterna i Europarådet och de övriga stater som är parter i konventionen om IT-relaterad brottslighet, som öppnades för undertecknande i Budapest den 23 november 2001, och har undertecknat detta protokoll,

som beaktar att Europarådets syfte är att skapa en fastare enhet mellan dess medlemmar, som erinrar om att alla människor är födda fria och jämbördiga i fråga om värdighet och rättigheter,

som betonar behovet av att säkerställa ett fullständigt och verkningsfullt förverkligande av mänskliga rättigheter utan någon diskriminering eller åtskillnad, såsom de garanteras i europeiska och andra internationella instrument,

som är övertygade om att gärningar av rasistisk och främlingsfientlig natur utgör en kränkning av de mänskliga rättigheterna och ett hot mot ett lagbundet samhällsskick och demokratisk stabilitet,

som anser att den nationella och den internationella rätten behöver tillhandahålla adekvata rättsliga åtgärder mot propaganda av rasistisk och främlingsfientlig natur som bedrivs med hjälp av datorsystem,

som är medvetna om att propaganda för sådana gärningar ofta är straffbelagd i nationell lagstiftning,

som beaktar konventionen om IT-relaterad brottslighet, som föreskriver moderna och flexibla medel för internationellt samarbete, och som är övertygade om behovet av att harmonisera materiella lagbestämmelser som rör kampen mot rasistisk och främlingsfientlig propaganda,

som är medvetna om att datorsystem erbjuder medel utan tidigare motstycke för att underlätta yttrandefrihet och frihet att meddela sig i hela världen,

som erkänner att yttrandefriheten är en av de viktigaste grundvalarna i ett demokratiskt samhälle och en av de grundläggande förutsättningarna för samhällets framåtskridande och varje människas utveckling,

som emellertid är oroade över risken för felaktig användning eller missbruk av sådana datorsystem för att sprida rasistisk och främlingsfientlig propaganda,

som är medvetna om behovet av att säkerställa en lämplig avvägning mellan yttrandefrihet och effektiv bekämpning av gärningar av rasistisk och främlingsfientlig natur,

som erkänner att detta protokoll inte avser att påverka redan etablerade principer om yttrandefrihet i nationella rättssystem,

som beaktar tillämpliga internationella rättsliga instrument på detta område, särskilt konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och dess protokoll nr 12 om allmänt förbud mot diskriminering, de befintliga Europarådskonventionerna om samarbete på det straffrättsliga området, särskilt konventionen om IT-relaterad brottslighet, Förenta nationernas internationella konvention om avskaffande av alla former av rasdiskriminering av den 21 december 1965, Europeiska unionens gemensamma åtgärd av den 15 juli 1996, som antogs av rådet med stöd i artikel K.3 i fördraget om Europeiska unionen, om åtgärder mot rasism och främlingsfientlighet,

som välkomnar den senaste utvecklingen som ytterligare främjar internationell förståelse och internationellt samarbete i fråga om bekämpning av IT-relaterad brottslighet och rasism och främlingsfientlighet,

som även beaktar den handlingsplan som antogs av Europarådets stats- och regeringschefer vid deras andra toppmöte i Strasbourg den 10–11 oktober 1997 för att söka gemensamma svar på utvecklingen av nya informationsteknologier, som grundar sig på Europarådets normer och värderingar,

har kommit överens om följande.

Kapitel I – Gemensamma bestämmelser

Artikel 1 – Syfte

Syftet med detta protokoll är att med avseende på parterna i protokollet komplettera bestämmelserna i konventionen om IT-relaterad brottslighet som öppnades för undertecknande i Budapest den 23 november 2001 (nedan kallad *konventionen*) vad gäller kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem.

Artikel 2 – Definition

1. I detta protokoll används denna definition:

rasistiskt och främlingsfientligt material: skrivet material, bild eller annan framställning av idéer eller teorier som förespråkar, främjar eller uppmuntrar till hat, diskriminering eller våld mot en enskild person eller en grupp av personer på grund av ras, hudfärg, härstamning, nationellt eller etniskt ursprung liksom även trosbekännelse, under förebärande av något av de förstnämnda karakteristika.

2. De termer och uttryck som används i protokollet 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.

Sammanfattning av departementspromemorian Brott och brottsutredning i IT-miljö. Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll (Ds 2005:6) i nu aktuell del

Bör konventionen och tilläggsprotokollet ratificeras?

Kapitel 9 behandlar frågan om konventionen respektive tilläggsprotokollet bör ratificeras.

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

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

Förteckning över remissinstanserna

Efter remiss har yttrande lämnats av Brottsförebyggande rådet, Datainspektionen, Domstolsverket, Ekobrottsmyndigheten, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Gävle tingsrätt, Göteborgs tingsrätt, Helsingborgs tingsrätt, Hovrätten för Nedre Norrland, Hässleholms tingsrätt, Integrationsverket, IT & Telecomföretagen, Justitiekanslern, Luleå tingsrätt, Nationellt foresiskt centrum, Ombudsmannen mot etnisk diskriminering, Polismynigheten, Post- och telestyrelsen, Riksdagens ombudsmän (JO), SIG Security, Statskontoret, Stockholms universitet (Juridiska fakulteten), Svea hovrätt, Svenska avdelningen av Internationella juristkommissionen, Svenskt Näringsliv, Sveriges advokatsamfund,Sveriges domareförbund, Svenska Tidningsutgivareföreningen, Säkerhetspolisen, Telia Company, Tullverket, Uppsalas universitet (Juridiska fakulteten) och Åklagarmyndigheten.

Följande remissinstanser har inte svarat eller angett att de avstår från att yttra sig: Centrum mot rasism, Stiftelsen Expo, Svenska Helsingforskommittén för Mänskliga Rättigheter och Tele 2.

Sammanfattning av betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39) i nu aktuella delar

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.

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 undertecknat 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.

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 §
	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 §.
	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 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.

Denna lag träder i kraft den 1 januari 2015.

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 §[1]	
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,
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.

[1] Senaste lydelse 2012:284.

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 §[2]

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 *7, 8* och *11* lämnas 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 *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 §[3]

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 om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, *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.

4 §[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,

[2] Senaste lydelse 2007:982.
[3] Senaste lydelse 2007:982.
[4] Senaste lydelse 2011:906.

– 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.

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.

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 §[1]	
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 §[2]	
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 kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	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.

16 d §[3]

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.

[1] Senaste lydelse 2012:127.
[2] Senaste lydelse 2012:285.
[3] Senaste lydelse 2012:127.

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

21 §[4]

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 kom-	4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk

[4] Senaste lydelse 2012:285.

munikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *och*	kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
5. begäran om utlämnande av uppgift om abonnemang enligt 22 § första stycket 2.	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.

22 §[5]

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	7. uppgift som avses i 20 § första stycket 1 till polismyndighet el-

[5] Senaste lydelse 2012:285.

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, *och*

8. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.

ler 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.

Denna lag träder i kraft den 1 januari 2015.

Förteckning över remissinstanserna

Efter remiss har yttrande lämnats av Bahnhof AB, Barnombudsmannen, Brottsförebyggande rådet, Datainspektionen, Diskrimineringsombudsmannen, Domstolsverket, ECPAT Sverige, Ekobrottsmyndigheten, Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Gävle tingsrätt, Göteborgs tingsrätt, Helsingborgs tingsrätt, Hovrätten för Västra Sverige, Hovrätten över Skåne och Blekinge, Hässleholms tingsrätt, IT & Telekomföretagen, Juliagruppen, Justitiekanslern, Kustbevakningen, Luleå tingsrätt, Länsstyrelsen i Stockholms län, Migrationsverket, Myndigheten för samhällsskydd och beredskap, Nationellt forensiskt centrum, Polismyndigheten, Post- och telestyrelsen, Riksdagens ombudsmän (JO), Rättighetsalliansen, Skatteverket, Statskontoret, Stockholms universitet (Juridiska fakulteten), Svenska Journalistförbundet, Sveriges advokatsamfund, Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Totalförsvarets forskningsinstitut, Tullverket, Uppsala universitet (Juridiska fakulteten) och Åklagarmyndigheten.

Yttrande har även lämnats av en privatperson och Stiftelsen för Internetinfrastruktur (Internetstiftelsen) och Lunds universitets institut för internetstudier (LUii).

Följande remissinstanser har inte svarat eller angett att de avstår från att yttra sig: Centrum mot rasism, Civil Rights Defenders, Föreningen Utgivarna, Netnod Internet Exchange i Sverige AB, SIG Security, Stiftelsen Expo, Svenska avdelningen av Internationella juristkommissionen, Svenska Tidningsutgivareföreningen, Svenskt Näringsliv, Sveriges Domareförbund, Tele2 AB och Telia Company.

Sammanfattning av promemorian Kompletterande förslag inför ett tillträde till Budapestkonventionen

Bilaga 8

Promemorians huvudsakliga innehåll

Promemorian utgör ett komplement till betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39). I promemorian lämnas förslag på ändringar som bedöms nödvändiga i lagen (2017:1000) om en europeisk utredningsorder. Förslagen innebär att en europeisk utredningsorder ska kunna avse ett föreläggande att bevara en viss lagrad uppgift. Utredningsordern ska även kunna omfatta en begäran om röjande av uppgift om vilka övriga tillhandahållare som deltagit i överföringen av ett meddelande.

Lagändringarna föreslås träda i kraft den 1 december 2020.

Promemorians lagförslag

Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 3 kap. 5 § samt 4 kap. 1 och 2 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 2 kap. 16 a § och 3 kap. 33 a §, och närmast före 2 kap. 16 a § och 3 kap. 33 a § två nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
4 §[1]	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken *eller* en åtgärd enligt 27 kap. 15 § samma balk,	4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § *eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 §* samma balk,
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,	
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, eller	
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.	
	2 kap.
	Föreläggande att bevara en viss lagrad uppgift
	16 a §

[1] Senaste lydelse 2020:67.

När en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har verkställts i den andra medlemsstaten får den som har förelagts åtgärden begära rättens prövning. För rättens prövning gäller 27 kap. 6 § första stycket samma balk.

Den tid en uppgift enligt 27 kap. 16 § andra stycket rättegångsbalken ska bevaras, räknas från den tidpunkt då åtgärden verkställdes i den andra medlemsstaten. Tiden får förlängas med ytterligare 90 dagar om det finns särskilda skäl.

3 kap.

5 §

En utredningsorder får inte erkännas och verkställas i Sverige om

1. det skulle strida mot bestämmelser om immunitet och privilegier eller om skydd för uppgifter som avses i 36 kap. 5 och 5 a §§ rättegångsbalken,

2. ordern avser beslag av en skriftlig handling eller ett skriftligt meddelande och det enligt 27 kap. 2 § rättegångsbalken finns hinder mot att ta handlingen eller meddelandet i beslag,

2. ordern avser beslag av en skriftlig handling eller ett skriftligt meddelande *eller ett föreläggande att bevara en viss lagrad uppgift* och det enligt 27 kap. 2 § rättegångsbalken finns hinder mot att ta handlingen eller meddelandet i beslag *eller enligt 27 kap. 16 § tredje stycket samma balk meddela ett föreläggande*,

3. det skulle medföra fara för Sveriges säkerhet, äventyra enskilda personers säkerhet eller medföra risk för röjande av uppgifter som rör underrättelseverksamhet,

4. den gärning som avses i utredningsordern har begåtts utanför den utfärdande medlemsstatens territorium och helt eller delvis i Sverige, och gärningen inte motsvarar ett brott enligt svensk lag, eller

5. utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 §.

En utredningsorder får inte vägras enligt första stycket 5, om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser.

Föreläggande att bevara en viss lagrad uppgift

33 a §

När en utredningsorder för ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har verkställts,

	tillämpas 32 § första, fjärde och femte styckena.
	Den tid en uppgift enligt 27 kap. 16 § andra stycket rättegångs-balken ska bevaras får förlängas med ytterligare 90 dagar om det finns särskilda skäl.

4 kap.

1 §

Domstolens beslut enligt 2 kap. 5, 14 *och* 16 §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *angående* den åtgärd som avses i utredningsordern.	Domstolens beslut enligt 2 kap. 5, 14*,* 16 *och 16 a* §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *om* den åtgärd som avses i utredningsordern.

Ett beslut i fråga om att utfärda en utredningsorder får inte överklagas.

2 §

Domstolens beslut enligt 3 kap. 9, 32 *och* 33 §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *angående* en åtgärd som motsvarar den åtgärd som avses i utredningsordern. Domstolens beslut enligt 3 kap. 25 § får överklagas på det sätt som gäller enligt rättegångsbalken.	Domstolens beslut enligt 3 kap. 9, 32*,* 33 *och 33 a* §§ får överklagas. Vid överklagande gäller vad som är föreskrivet i rättegångsbalken eller annan författning för beslut *om* en åtgärd som motsvarar den åtgärd som avses i utredningsordern. Domstolens beslut enligt 3 kap. 25 § får överklagas på det sätt som gäller enligt rättegångsbalken.

Övriga beslut i fråga om erkännande och verkställighet av en utredningsorder får inte överklagas.

Denna lag träder i kraft den 1 december 2020.

Förteckning över remissinstanserna

Efter remiss har yttrande lämnats av Datainspektionen, Ekobrottsmyndigheten, Helsingborgs tingsrätt, Hovrätten för Västra Sverige, IT & Telekomföretagen, Justitiekanslern, Polismyndigheten, Post- och telestyrelsen, Riksdagens ombudsmän (JO), Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Tullverket, Uppsala universitet (Juridiska fakulteten), Sveriges advokatsamfund och Åklagarmyndigheten.