Stockholm den 20 september 2013

R-2013/1044

Till Justitiedepartementet

Ju2013/4173/Å

Sveriges advokatsamfund har genom remiss den 1 juli 2013 beretts tillfälle att avge yttrande över betänkandet Europarådets konvention om IT-relaterad brottslighet (SOU 2013:39).

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

## Sammanfattning av Advokatsamfundets synpunkter

Sverige har ratificerat konventionen och tilläggsprotokollet, men ännu ej undertecknat desamma. Till vissa delar är förslagen i betänkandet nödvändiga för att uppfylla Sveriges skyldigheter enligt konventionen, tilläggsprotokollet och det kommande direktivet.

Advokatsamfundet avstyrker trots detta att huvuddelen av förslagen läggs till grund för lagstiftning.

Advokatsamfundet gör även andra bedömningar än utredningen beträffande olika frågor och har synpunkter i övrigt på förslagen enligt vad som framgår i det följande.

Advokatsamfundet har ingen erinran mot ett införande av brottet grovt dataintrång, men har samtidigt synpunkter på förslagets kongruens med annan lagstiftning.

**Några allmänna synpunkter på utredningens förslag**

Advokatsamfundet delar utredningens uppfattning om datasystemens stora betydelse för samhället och har, även beaktat den därpå följande möjligheten att använda straff-processuella tvångsmedel, ingen erinran mot förslaget om att införa ”grovt dataintrång” med en åtföljande skärpning av straffskalan. En sådan straffskärpning skulle då även motsvara informationssystemsdirektivets krav på straffbestämmelser.

Advokatsamfundet ifrågasätter emellertid varför utredningen inte föreslagit motsvarande ändringar även beträffande övriga informationsintrångsbrott i 4 kap. brottsbalken (BrB). Samma skäl för en strängare straffskala för grovt dataintrång kan rimligen anläggas också på dessa brott. Särskilt gäller detta brytande av post- eller telehemlighet, eftersom nät och tjänster för elektronisk kommunikation också är av mycket stor betydelse för samhället och där det inte alltid är lätt att skilja mellan information som förekommer i samband med datorer och som är föremål för elektronisk kommunikation. Datorer ingår i och kommunicerar i mycket hög grad via elektroniska kommunikationsnät och tjänster. Genom teknikneutrala bestämmelser skulle vidare onödiga diskussioner kunna undvikas om vilken teknik som använts för att därigenom hänföra brottet till den ena eller andra rubriceringen.

Förslaget har inte heller i tillräcklig grad beaktat att egenskaperna och förutsättningarna för informationstekniken varierar stort. Med hänsyn härtill vill Advokatsamfundet peka på risken att rättstillämpningen kan komma att överskatta värdet och tillförlitligheten hos de elektroniska uppgifter som förekommer och som ska åberopas som bevisning, vilket i sin tur kan leda till oriktiga domar och beslut. Denna fråga blir särskilt viktig om det nu blir fråga om en så väsentlig skärpning av straffskalorna som föreslås.

Advokatsamfundet anser att den proportionalitetsavvägning som ligger till grund för vissa av förslagen inte i tillräcklig grad har beaktat de konventionsskyddade fri- och rättig-heterna, varför de föreslagna möjligheterna att förelägga om bevarande av uppgifter, liksom om att lämna upplysningar om ett datasystem, har blivit alltför ingripande för att kunna anses nödvändiga eller lämpliga för att uppfylla de ändamål som ligger bakom förslagen.[1]

Advokatsamfundet har inte heller funnit någon övertygande argumentation om hur eller varför de föreslagna möjligheterna att förelägga om bevarande eller att lämna upplysning om datasystem skulle leda till någon påtaglig förbättring av möjligheterna till framgång i

[1] Artikel 8.1, Europakonventionen för de mänskliga fri- och rättigheterna.

utredningarna. Det saknas exempelvis redogörelse för fall där utredningarna misslyckats på grund av att myndigheterna saknar möjligheten att använda föreslagna förelägganden och där den uteblivna framgången inte berott på andra orsaker. Det finns enligt Advokatsamfundets uppfattning därför inget som tyder på att nyttan med förslagen skulle bli annan än marginell och därmed väger fördelarna inte över de nackdelar som förslagen innebär bl.a. för den personliga integriteten, rätten till skydd för privat- och familjeliv och rättssäkerhet. Advokatsamfundet anser därför att de föreslagna åtgärderna i dessa hänseenden varken kan anses effektiva eller nödvändiga vare sig för att uppfylla konventionens krav eller för att förbättra brottsutredningarna.

Advokatsamfundet finner det särskilt betänkligt att förelägganden ska kunna riktas mot vem som helst, även privatpersoner. Detta kan enligt Advokatsamfundets uppfattning försätta den enskilde i mycket svåra och obehagliga situationer, t.ex. om hon eller han därigenom försätts i lojalitetskonflikter med den person som är av intresse i den utredning som föranlett föreläggandet.

Det finns heller inget i förslaget som uttryckligen begränsar möjligheten att förelägga om bevarande eller att lämna upplysning om datasystem i de fall där de uppgifter som omfattas av föreläggandena skulle omfattas av sekretess eller tystnadsplikt hos den som är föremål för föreläggandet. Inte heller det grundlagsfästa källskydd som skyddar kommunikation mellan t.ex. journalister och deras uppgiftslämnare är uttryckligen undantaget. Från Advokatsamfundets perspektiv är förslaget om bevarandeföreläggande än mer betänkligt, eftersom det även kan medföra en inskränkning av advokatsekretessen. De föreslagna reglerna innehåller nämligen heller ingen uttrycklig begränsning vad gäller uppgift om eller innehållet i kommunikation mellan försvararen och dennes klient. Om advokater åläggs att spara information om sina klienter kan detta skada den förtrolighet mellan advokaterna och deras klienter som enligt rättsstatens principer och kravet på rättssäkerhet måste råda, inte minst i advokaternas roll som försvarare.

Att utredningen förutsätter att de brottsutredande myndigheterna, t.ex. på grund av proportionalitetsprincipen, inte kommer att tillgripa föreläggandena i dessa fall är självfallet inte tillfredsställande. Det borde därför tydligt framgå direkt i de föreslagna bestämmelserna att föreläggandena inte får tillgripas i den mån det följer av andra bestämmelser att myndigheten inte får inhämta de uppgifter som omfattas av föreläggandet. På så sätt skulle därmed den i lag fastslagna advokatsekretessen kunna bibehållas.

Advokatsamfundet har tidigare uttryckt sin djupa oro över implementeringen av trafik-datalagringsdirektivet och dess konsekvenser.[2] När det nu föreslås något som liknar angiveriplikt för enskilda, finner Advokatsamfundet att rättsutvecklingen på området är mycket oroväckande. Den nytta samhället kan ha av de föreslagna åtgärderna kan inte vara värd priset av det kontroll- och angiverisamhälle med den misstänksamhet mellan medborgare och samhälle som åtgärderna i värsta fall kan komma att leda till. Dylika

[2] Se Advokatsamfundets remiss den 13 mars 2008, R-2008/0035.

former av medborgarskyldigheter att samarbeta med brottsbekämpande myndigheter är förkastliga och har ingenting att göra i en rättsstat.

Advokatsamfundet ser nu också med ännu större oro på den rådande rättsutvecklingen inom området. Det går enligt Advokatsamfundets uppfattning inte att bedöma utredningens förslag isolerat för sig, utan de föreslagna lagändringarna måste ses i ett större sammanhang. Skyldigheten för operatörerna att anpassa sina nät och tjänster för elektronisk kommunikation för att möjliggöra tvångsmedel för inhämtande av information i utredningarna har återkommande följts av nya liknande tillskott i lagstiftningen. Som exempel på sådana ytterligare lagstiftningsåtgärder kan nämnas ändringarna i upphovsrättslagen enligt IPRED och införandet av trafikdatalagringsskyldigheten. Operatörer och tjänsteleverantörer har på detta sätt alltmer kommit att bli redskap för myndigheterna för att övervaka och kontrollera medborgarna. Utredningens förslag är i berörda delar ytterligare steg i denna utveckling, där den enskildes privata sfär och rätt att bli lämnad i fred från myndigheternas insyn krymper alltmer. Det finns ingen anledning att tro att utredningens förslag blir den sista byggstenen, utan framtiden kommer att innehålla återkommande lagstiftningsinitiativ som fortsätter inskränka den enskildes integritet så att det till slut inte finns något kvar. Att lagstiftningsförslagen är av stringent juridisk teknisk natur är i ett sådant sammanhang en klen tröst. Det blir lite som att ”operationen gick jättebra, men patienten dog”.

**Några särskilda synpunkter kring proportionalitet, rättssäkerhet och integritet**

Utredningens utgångspunkt har varit att lämna förslag till lagstiftningsåtgärder för att Sverige ska kunna uppfylla sina åtaganden enligt Europarådets konvention om IT-relaterad brottslighet, dess tilläggsprotokoll jämte Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF. Det primära syftet med detta är att de brottsutredande myndigheterna ska ha tillgång till effektiva redskap att utreda och beivra brott. Detta innebär en risk för att rättssäkerheten och integritetsaspekterna, samt den enskildes rätt att få vara i fred, fått en sekundär betydelse i utredningens arbete med att ta fram lämpliga författningsförslag. Att så är fallet framgår inte minst av att en övervägande del av utredningen handlar om lagtekniska resonemang eller resonemang kring hur Sveriges internationella åtaganden på lagstiftningsområdet ska uppfyllas och endast i obetydlig omfattning diskuterar rättssäkerhets- och integritetsaspekterna.

Sverige har i och för sig ett åtagande att genomföra de lagstiftningsåtgärder som krävs för att uppfylla konventionen och tilläggsprotokollet. Men trots konventionen och tilläggsprotokollet gäller Europakonventionen om de mänskliga fri- och rättigheterna. De lagstiftningsåtgärder som föreslås måste därför ske på sätt att åtgärderna inte får ett tillämpningsområde som blir större än vad som är nödvändigt för att tillgodose de ändamål som ligger till grund för de föreslagna bestämmelserna. Lagstiftningsåtgärderna måste uppfylla de minimikrav på straffprocessuella tvångsmedel som följer av Europakonventionen för de mänskliga fri- och rättigheterna och av regeringsformen. Det ska således föreligga ett behov av åtgärderna, de ska vara effektiva och de ska vara

proportionerliga. Advokatsamfundet anser att de föreslagna åtgärderna i många delar är synnerligen ingripande för den enskilde, särskilt som denne genom det föreslagna bevarandeföreläggandet kommer att kunna uppleva sig vara tvingad att direkt eller indirekt fungera som en angivare åt myndigheterna och dessutom under tystnadsplikt.

Rättsutvecklingen har inneburit att myndigheterna i allt större utsträckning kan få tillgång till verktyg för att övervaka medborgarna. Operatörer är sedan 1999 skyldiga att välja en teknik och utforma sina nät och tjänster för elektronisk kommunikation så att hemlig avlyssning eller övervakning av elektronisk kommunikation kan genomföras. I denna skyldighet ingår även att tillhandahålla de brottsutredande myndigheterna nätanslutningspunkter där dessa åtgärder kan ske.[3] Sedan 2012 är operatörer skyldiga att lagra trafikdata i sex månader.[4] Med dessa verktyg borde myndigheterna ha tillgång till tillräcklig information för att kunna framgångsrikt bedriva brottsutredningarna. Men enligt förslaget ska alla, t.o.m. enskilda personer, vara skyldiga att spara information.

Mot denna bakgrund kan Advokatsamfundet inte se att det därutöver skulle finnas ett rimligt behov av att ytterligare utöka myndigheternas tillgång till uppgifter och kontroll i den omfattning som förslaget innebär.

De föreslagna åtgärderna innefattar således väsentliga intrång i enskilda människors rätt till respekt för sitt privatliv och sin korrespondens. Bevarandeföreläggandet kommer att kunna tillgripas oberoende av vilket slags brott det är fråga om. Inte ens advokaters klientsekretess kommer att utgöra ett hinder mot ett föreläggande. Förslaget är därmed enligt Advokatsamfundets uppfattning inte proportionerligt i förhållande till de inskränkningar i integritetsskyddet som kommer att bli följden. Samhällets intresse i och behov av detta långtgående förslag kan rimligen inte heller uppväga den olägenhet som det innebär för en enskild att enligt förslaget mot sin vilja tvingas spara information om sina kontakter på ett sätt som försätter denne i en position som angivare.

Advokatsamfundet är av den bestämda uppfattningen att myndigheterna i tillräckligt hög grad får anses vara garanterade tillgång till information genom operatörernas skyldighet att anpassa nät och tjänster för att möjliggöra verkställande av hemlig avlyssning eller övervakning av elektronisk kommunikation, kombinerat med dessa aktörers skyldighet att lagra trafikdata. Det finns därmed inget behov av att utsträcka dessa skyldigheter även till enskilda personer.

## Synpunkter på de föreslagna ändringarna i rättegångsbalken

*Bevarandeföreläggande*

Enligt förslaget ska undersökningsledare eller åklagare kunna meddela ett föreläggande om att bevara uppgifter i elektronisk form, som skäligen kan antas ha betydelse i en utredning. Föreläggandet ska enligt förslaget få riktas mot inte bara tjänsteleverantörer

[3] 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation, infördes genom lag (1999:578).
[4] 6 kap. 16 a §§ lagen (2003:389) om elektronisk kommunikation.

eller operatörer, utan även mot andra. Således kan bevarandeföreläggande komma att riktas mot andra juridiska personer och t.o.m. även mot privatpersoner. Föreläggandet ska vidare enligt förslaget kunna omfatta alla slags elektroniskt lagrade uppgifter, vilket enligt Advokatsamfundet måste anses omfatta all trafikdata och även innehållet i de kommunikationer som finns sparade hos den som föreläggs.[5] Skyldigheten att följa föreläggandet kommer att vara straffsanktionerad och det föreslås även att den som föreläggandet riktas mot ska omfattas av en straffsanktionerad tystnadsplikt avseende åtgärden.[6]

Enligt Advokatsamfundets uppfattning innebär förslaget i denna del ett oacceptabelt införande av skyldigheter för företag och enskilda att bistå de brottsutredande myndigheterna. Advokatsamfundet är mycket kritiskt till förslaget inte bara för att det i sig är fråga om långtgående skyldigheter för den enskilde och andra, utan även för att förslaget om det skulle genomföras innebär ytterligare ett exempel på där enskilda och företag åläggs att agera som angivare och att hjälpa polis och åklagare att effektivisera den brottsbekämpande verksamheten.

Samtidigt innebär förslaget att bevarandeskyldigheten går längre än de undantag från vittnesplikten som enligt gällande regler föreskrivs i rättegångsbalken (RB). Enligt förslaget begränsas möjligheten att besluta om bevarandeföreläggandet endast på så sätt att det inte får riktas mot den misstänkte själv eller någon denne närstående som anges i 36 kap. 3 § RB. När det gäller föreläggande om uppgiftsskyldighet avseende personer som har särskild kännedom om ett datasystem, ska dock begränsningarna i vittnesplikten enligt förslaget gälla fullt ut.[7] Detta ska tydligen uppfattas som att övriga inskränkningar i vittnesplikten enligt RB inte ska gälla vid bevarandeföreläggande.

De föreslagna bestämmelserna innebär därmed att en försvarare skulle kunna föreläggas att bevara alla uppgifter om sin klient kommunikationen och även innehållet i kommunikationen mellan advokaten och klienten.[8] Förslaget innebär därmed en allvarlig urgröpning av det skydd för förtroligheten mellan försvararen och klienten som hittills gällt och ansetts grundläggande för såväl advokatens roll i rättssamhället som för rättsstaten som sådan. Enligt Advokatsamfundet är det helt enkelt orimligt att ett sådant förslag skulle få genomslag i svensk lagstiftning.

Advokatsamfundet är medvetet om att vissa andra bestämmelser ändå skulle kunna hindra myndigheterna från att få tillgång till de bevarade uppgifterna. Detta är självfallet dock inget skäl för att det skulle föreligga ett behov av en bestämmelse som ändå medger ett bevarandeföreläggande även i sådana fall. Det skulle i så fall dessutom innebära att ett föreläggande om bevarande av uppgifter skulle bli meningslöst, vilket inte kan anses förenligt med en tydlig och förutsägbar lagstiftning. Men då finns det ju inte ett behov.

[5] Se SOU 2013:39 s. 329 ff.
[6] SOU 2013:39 s. 331 f.
[7] SOU 2013:39 s. 333.
[8] Undantag från vittnesplikten föreligger i dessa fall enligt rättegångsbalken 36 kap. 5 §.

Enligt Advokatsamfundets förmenande är det under föreliggande förutsättningar nödvändigt att i bestämmelsen uttryckligen ange att föreläggandet inte får tillgripas i de fall där det följer av andra bestämmelser att myndigheten inte får inhämta de uppgifter som omfattas av föreläggandet.

Bevarandeföreläggganden kommer även att kunna riktas mot operatörer avseende uppgifter som hos dessa omfattas av tystnadsplikt.[9] Rätten för myndigheterna att trots denna tystnadsplikt få tillgång till dessa uppgifter är närmare reglerad på olika håll i lagstiftningen. Trafikuppgifter kan trots tystnadsplikten inhämtas av myndigheterna enligt reglerna om hemlig övervakning av elektronisk kommunikation och uppgifter om innehållet i elektroniska meddelanden enligt reglerna om hemlig avlyssning av elektronisk kommunikation.[10] Om nu myndigheterna inte kommer att kunna få tillgång till uppgifterna på grund av begränsningar i andra bestämmelser, finns det heller ingen anledning till att den föreslagna bestämmelsen till sin lydelse ska möjliggöra ett bevarandeföreläggande i dessa fall. Advokatsamfundet anser därför att det inte heller i detta avseende kan vara förenligt med proportionalitetsprincipen att införa en bestämmelse med angiven innebörd. Även på denna grund anser Advokatsamfundet det vara nödvändigt att i bestämmelsen uttryckligen ange att föreläggandet inte får tillgripas i de fall där det redan följer av andra bestämmelser att myndigheten inte får inhämta de uppgifter som omfattas av föreläggandet.

En annan situation där ett bevarandeföreläggande enligt den föreslagna bestämmelsen skulle kunna tillgripas där myndighetens tillgång till uppgifterna begränsas, är när uppgiften omfattas av det grundlagsfästa källskyddet för journalisters uppgiftslämnare. Lydelsen i den föreslagna bestämmelsen möjliggör därmed för myndigheterna att förelägga om bevarande av kommunikation mellan journalister och deras källor, trots att dessa uppgifter enligt Tryckfrihetsförordningen (TF) inte får vara föremål för myndigheternas efterforskning.[11] Eftersom myndigheterna därmed inte kan få tillgång till uppgifterna, skulle det bli meningslöst med ett bevarandeföreläggande även i denna situation. Även av detta skäl anser Advokatsamfundet det vara nödvändigt att i bestämmelsen uttryckligen ange att föreläggandet inte får tillgripas i de fall där det följer av andra bestämmelser att myndigheten inte får inhämta de uppgifter som omfattas av föreläggandet.

Ett bevarandeföreläggande ska vidare enligt förslaget inte få riktas mot den misstänkte själv eller någon denne närstående som anges i 36 kap. 3 § RB. Detta är också det enda uttryckliga undantaget som det hänvisas till i den föreslagna bestämmelsen. Till sin lydelse innebär den föreslagna bestämmelsen att föreläggandet får meddelas i alla övriga fall där undantag från vittnesplikten föreligger enligt 36 kap. RB, t.ex. undantagen i 36 kap. 5 § RB.

[9] Lagen (2003:389) om elektronisk kommunikation, 6 kap. 20 §.
[10] 27 kap. 18 och 19 §§ rättegångsbalken.
[11] Tryckfrihetsförordningen 3 kap. 4 §.

När det gäller ett föreläggande om att lämna upplysning om ett datasystems funktioner när detta behövs för att ett beslut om husrannsakan ska kunna verkställas, ska enligt förslaget dock samtliga undantag från vittnesplikten i 36 kap. RB hindra ett sådant föreläggande. Följden av detta torde bli att uppgifter kan tillgripas genom husrannsakan och beslag om åtgärden sker efter ett bevarandeföreläggande, men inte om åtgärden sker efter ett föreläggande om att lämna upplysning om ett datasystems funktioner. Enligt Advokatsamfundet skulle det bli både inkonsekvent och oförutsägbart om inte samma förutsättningar gäller för båda dessa typer av förelägganden. Enligt Advokatsamfundet är det nödvändigt att i bestämmelsen uttryckligen ange att inget av föreläggandena får tillgripas i de fall där något undantag från vittnesplikten föreligger enligt 36 kap. RB.

Beträffande möjligheten att rikta ett bevarandeföreläggande även mot enskilda personer, har anförts att nyttan med ett sådant föreläggande kommer att vara mycket begränsad. Det finns ingen uppgift om hur ofta sådana förelägganden förekommit i de länder som infört motsvarande bestämmelse och inte heller vilken nytta som kan förväntas med bestämmelsen. Även om det av olika skäl skulle kunna antas att förelägganden mot enskilda personer kommer att bli mycket sällsynta, ingår möjligheten trots allt i den föreslagna bestämmelsen. Om det i praktiken sedan anses att det inte kommer riktas några bevarandeförelägganden mot enskilda personer,[12] är det enligt Advokatsamfundet svårt att förstå varför en bestämmelse med sådan innebörd överhuvudtaget måste införas. Advokatsamfundet motsätter sig därför förslaget även i denna del.

Advokatsamfundet ställer sig även tveksamt till om möjligheten att rikta ett bevarandeföreläggande verkligen skulle leda till någon nytta i den brottsutredande verksamheten. Det borde i så fall ha kunnat redovisas fall eller statistik över fall där utredningar stått och fallit med tillgången på sådana uppgifter som avses kunna omfattas av ett bevarandeföreläggande, och där utredningarna inte kunnat drivas vidare på grund av att sådana uppgifter inte kunnat inhämtas. Några sådana siffror redovisas inte i förslaget.

Bevarandeföreläggande ska kunna ske redan på sådant stadium i utredningen att det ännu inte föreligger någon misstänkt, oberoende av brottets svårighetsgrad och det ska räcka med att uppgiften ”skäligen kan antas ha betydelse”.[13] Detta betyder att det enligt förslaget inte ska krävas särskilt mycket för att bevarandeföreläggande ska få tillgripas, trots att åtgärden är långtgående och ingripande för de enskilda. Dessutom begränsas inte åtgärden till de allvarliga brotten, utan bevarandeföreläggandet kan enligt den föreslagna bestämmelsens lydelse komma att tillgripas även vid lindrig brottslighet som t.ex. snatteri. En annan omständighet av betydelse är att de uppgifter som ska kunna bli föremål för ett bevarandeföreläggande förekommer i datorer eller system där skyddet mot obehörig åtkomst eller andra säkerhetsåtgärder kan antas vara av varierande kvalitet. Därav följer att säkerheten och tillförlitligheten kommer att vara olika hos de uppgifter som inhämtas från olika användare. Om tillförlitligheten hos uppgifterna övervärderas, innebär detta en påtaglig risk för att de uppgifter som inhämtas efter ett bevarandeföreläggande leder till

[12] SOU 2013:39 s. 317.
[13] SOU 2013:39 s. 330 f.

oriktiga domar och beslut.[14] Osäkerheten beträffande tillförlitligheten hos uppgifterna innebär enligt Advokatsamfundet att myndigheternas intresse och behov av att kunna få tillgång till dem har överskattats i förslaget. Åtminstone torde intresset och behovet av dessa skäl vara betydligt mindre när det gäller enskilda, där säkerheten och tillförlitligheten hos uppgifterna kan vara än mer diskutabla. Detta utgör enligt Advokatsamfundet ytterligare skäl för att avstyrka att bestämmelsen möjliggör ett bevarandeföreläggande mot enskilda personer.

Det finns i sammanhanget även anledning erinra om att någon uppgiftsskyldighet för den förelagde gentemot den föreläggande myndigheten inte föreslås. Om den som föreläggs att bevara uppgifter samtidigt omfattas av sekretess eller tystnadsplikt enligt lag för de uppgifter som omfattas av föreläggandet, kan denne därigenom samtidigt vara förhindrad att tillmötesgå den brottsutredande myndigheten genom att faktiskt överlämna uppgifterna eller på annat sätt aktivt göra dem tillgängliga för myndigheten.[15] En husrannsakan och ett beslag innefattar i sig ingen uppgiftsskyldighet för den som omfattas av åtgärden och utgör heller ingen sådan omständighet som gör ett överlämnande, dvs. ett röjande av uppgiften, behörigt. Husrannsakan och beslag får t.ex. inte användas för att kringgå operatörernas tystnadsplikt när det gäller trafikuppgifter om elektroniska meddelanden.[16] Den förelagde är emellertid av praktiska skäl ofta tvingad att bistå myndigheten genom att lämna ut uppgifterna, bl.a. för att undvika att myndigheten orsakar skada i systemen vid verkställandet av beslaget. Även om det finns vissa regler som hindrar myndigheten från att ta uppgifter i beslag, utesluter inte detta att myndigheten tar emot uppgifter som ”frivilligt” lämnas ut även om ett samtycke till tvångsmedel saknar verkan.[17]

På detta sätt kan förslaget därför enligt Advokatsamfundet leda till ökad risk för att den förelagde i praktiken känner sig tvingad att obehörigen åsidosätta sin sekretess eller tystnadsplikt. Denna problematik kan i och för sig undanröjas genom att myndigheten samtidigt meddelar föreläggande att lämna upplysning om ett datasystems funktioner för att myndigheten därefter själv kan genomföra husrannsakan och beslag avseende uppgifterna. Advokatsamfundet anser dock att det i de föreslagna bestämmelserna uttryckligen bör anges att den som följer ett föreläggande inte samtidigt kan anses ha åsidosatt sin sekretess eller tystnadsplikt.

Sammantaget anser Advokatsamfundet att det i bestämmelsen om bevarandeföreläggande uttryckligen ska anges att föreläggandet inte får tillgripas i de fall där det följer av andra bestämmelser att myndigheten inte får inhämta de uppgifter som omfattas av föreläggandet. Advokatsamfundet anser även att det i de föreslagna bestämmelserna uttryckligen anges att den som följer ett föreläggande inte anses ha åsidosatt sin sekretess eller tystnadsplikt. Beträffande de föreslagna bestämmelserna om bevarandeföreläggande anser Advokatsamfundet att det inte är förenligt med proportionalitetsprincipen att

[14] Jfr t.ex. Svea hovrätts dom, 2006-10-02, mål nr B 8799-05.
[15] SOU 1992:110 s. 335 f. om ”aktiv medverkan”.
[16] Se RH 1999:97.
[17] SOU 2013:39 s. 196.

bevarandeföreläggande ska kunna riktas även mot enskilda personer, varför samfundet motsätter sig detta förslag.

*Föreläggande att lämna upplysning om datasystemets funktioner*

Detta förslag innebär att det ska vara möjligt att förelägga en person som har kunskap om ett visst datasystem att lämna upplysning om datasystems funktioner när detta behövs för att ett beslut om husrannsakan ska kunna verkställas.

Advokatsamfundet får i sammanhanget framhålla att det finns ett berättigat intresse i att myndigheterna inte själva bereder sig tillgång till andras datasystem och att utredningarna så långt möjligt bedrivs på ett sätt som inte riskerar att skada systemen eller uppgifterna som finns lagrade i systemen. Eftersom det ligger i systemägarens intresse att systemet eller uppgifterna inte skadas, har denne i de flesta fall ett intresse av att medverka till åtgärdernas genomförande. Samtidigt är det systemägaren som är bäst lämpad att bedöma vilka personer som har kunskap om systemet och vilka som är kvalificerade. Därför borde föreläggandet inte få meddelas förrän den som äger eller svarar för systemet först har beretts tillfälle att själv utse lämplig person som bistår myndigheten. Utan denna möjlighet blir det den som myndigheten förelägger som kommer att vara tvungen att biträda myndigheten, även om det skulle visa sig att det finns andra personer med bättre kunskaper om systemet och som systemägaren hellre skulle ha anvisat.

Det kan uppstå intresse- och lojalitetskonflikter om föreläggandet syftar till att myndigheten ska få tillgång till uppgifter i en utredning som riktar sig mot den förelagdes arbetsgivare eller kollegor. De undantag som föreslås, dvs. undantagen från vittnesplikten i RB, omfattar nämligen generellt sett inte dem. Det kan därför antas föreligga risk för att det på olika sätt kommer fram till den förelagdes arbetsgivare eller kollegor att föreläggandet meddelats, trots den tystnadsplikt som enligt förslaget ska gälla för den förelagde. Därmed är det enligt Advokatsamfundets uppfattning klart olämpligt att föreläggandet kommer att tillgripas i en situation där utredningen riktas mot någon hos den som äger eller disponerar systemet.

Precis som i fråga om förslaget till ett bevarandeföreläggande, aktualiserar också denna bestämmelse frågor rörande sekretess och tystnadsplikt för de berörda uppgifterna. Den information som myndigheten får tillgång till kan samtidigt omfattas av sekretess eller tystnadsplikt hos systemägaren. Genom att systemägaren eller dennes personal på olika sätt bistår myndigheten med upplysningar om hur myndigheten ska få tillgång till systemet eller viss information däri, kan det anses som att uppgiften aktivt lämnas ut av systemägaren eller någon hos denne. Detta kan i sin tur leda till osäkerhet om den förelagde i vissa fall rentav kan anses ha åsidosatt sin sekretess eller tystnadsplikt. Det anges inte i de föreslagna bestämmelserna om ett föreläggande undanröjer en eventuell sekretess eller tystnadsplikt avseende den information som ska åtkommas, vilket Advokatsamfundet anser utgör en brist i förslaget.

Så länge de åtgärder som den förelagde personen ska bidra med begränsas till att uppge lösenord och annat som behövs för att myndigheten ska få tillgång till begärda uppgifter, blir den förelagdes skyldighet att medverka i och för sig relativt begränsad. Den som föreläggs skulle i allmänhet även vara skyldig att med de begränsningar som anges i 36 kap. RB vittna om de uppgifter som hon eller han har tillgång till och som rör systemet eller uppgifter däri. Emellertid framstår det som onaturligt och främmande att någon hos systemägaren, som senare eventuellt ska bli föremål för tvångsmedlen husrannsakan och beslag, genom föreläggandet åläggs en skyldighet att *aktivt* medverka till tvångsmedlens genomförande. Tvärtom är det naturligt i en rättsstat att tvångsmedel genomförs utan krav på att den som utsätts ska vara aktivt behjälplig med genomförandet därav. Mot denna bakgrund är det mest naturligt att myndigheten genomför tvångsmedlen och att system-ägaren eller dennes personal endast förväntas bidra med en *passiv* medverkan, dvs. att genomförandet accepteras och inte hindras. I Datastraffrättsutredningen intogs den ståndpunkten att husrannsakan och beslag var sådana slags tvångsmedel där det förväntades en passiv medverkan, ett synsätt som fortfarande får anses vara rådande.[18]

Sammantaget motsätter sig Advokatsamfundet förslaget om att den som har kunskap om ett datasystem ska kunna föreläggas att bistå de brottsutredande myndigheterna med upplysningar som behövs för att myndigheten ska kunna göra husrannsakan och beslag i systemet.

*Särskilt om husrannsakan och beslag av elektroniska handlingar*

Advokatsamfundet vill i detta sammanhang även peka på att nuvarande regler om husrannsakan och beslag inte uttryckligen medger att dessa åtgärder verkställs i en elektronisk miljö. Enligt ordalydelsen i bestämmelserna får beslag göras endast avseende föremål eller *skriftlig* handling.[19] Informationen i ett datorsystem kan inte anses utgöra vare sig föremål eller skriftlig handling, utan är snarare att anse som en upptagning.[20] Detta innebär att husrannsakan och beslag avseende elektroniskt lagrade uppgifter i nuläget sker enligt en extensiv tolkning eller efter en analogi med ”skriftliga” handlingar av de ifrågavarande straffprocessuella bestämmelserna. Enligt Advokatsamfundets uppfattning är det önskvärt att i bestämmelserna i RB uttryckligen ange och förtydliga om även elektroniskt lagrade uppgifter ska kunna tas i beslag.[21] Detta kan t.ex. ske genom att beslag inte begränsas till att kunna ske avseende enbart föremål eller skriftlig handling, utan enkelt genom att ordet ”skriftlig” tas bort så att alla slags handlingar omfattas av regleringen.

[18] Jfr SOU 1992:110 s. 335 f. bl.a. om passiv eller aktiv medverkan.
[19] Se 27 kap. 1 § och 28 kap. 1 § RB.
[20] Se 2 kap. 3 § TF.
[21] Ds 2005:6 s. 283 f., jfr SOU 1995:47 s. 184 och 493 f. samt även JK:s beslut 2008-08-15, dnr 6545-06-21. Se även Advokatsamfundets riktlinjer ang. externa IT-tjänster vid advokatverksamhet, cirkulär nr 18/2011.

## Synpunkter på de föreslagna ändringarna i brottsbalken

*Grovt dataintrång*

Advokatsamfundet har inget att erinra mot att det införs en bestämmelse om grovt dataintrång. Liknande bestämmelser finns redan när det gäller t.ex. grovt (dator)bedrägeri[22] och grovt företagsspionerі[23]. En bestämmelse om grovt dataintrång skulle även kunna vara tillämplig om någon olovligen berett sig tillgång till klient-uppgifter hos en advokat. Hos advokater gäller nämligen en särskild bestämmelse om tystnadsplikt och advokater är i vissa sammanhang även undantagna från vittnesplikten.[24] Således tillmäts i lagstiftningen uppgifter hos advokater sådan betydelse att det torde kunna anses som särskilt allvarligt och därmed kunna bli fråga om ett grovt brott om ett dataintrång omfattar sådana uppgifter eller datorsystem hos advokater där sådana uppgifter ingår. Därtill torde det ligga i rättsstatens intresse och därmed även utgöra ett viktigt samhällsintresse att advokatsekretessen skyddas.[25] Det föreslagna straffstadgandet skulle därmed kunna utgöra ett förstärkt skydd för de uppgifter som omfattas av advokat-sekretessen, varför Advokatsamfundet ställer sig bakom förslaget i sig. Advokatsamfundet vill dock särskilt peka på följande effekter om förslaget genomförs.

*Behovet av kunskaper inom IT-området*

Om det införs en ny rubricering för grovt dataintrång, med åtföljande straffskärpning, ställer detta samtidigt nya och stora krav på att alla företrädare för rättsväsendet, som på något sätt arbetar med IT-relaterad brottslighet, har goda IT-kunskaper. Det blir särskilt angeläget att den utredning som sker hos polis och åklagare bedrivs av sådan personal och med sådana tekniska verktyg att garantierna för undvikande av oriktiga domar stärks. Motsvarande gäller i minst lika hög grad för advokater och försvarare. Försvarare måste så tidigt som möjligt få tillgång till sådant material som innehåller bevisning av IT-natur och även anlita specialister som har kunskap att förstå, granska och ifrågasätta materialet. Det måste även finnas förstärkta möjligheter för den misstänkte att få sina kostnader för bevisningen inklusive anlitade specialister täckta av samhället.

Av naturliga skäl blir effekterna av oriktiga domar och andra domstolsavgöranden särskilt påtagliga i de fall där det införts strängare påföljder och längre fängelsestraff. Samtidigt är IT-bevisningen ofta komplex, komplicerad och omfattande. Av dessa skäl finner Advokatsamfundet det angeläget att försvarare på ett mycket tidigt stadium kan få del av den IT-bevisning som föreligger i utredningen för att få tillräcklig tid för att bedöma materialet. Det måste även ges rimligt utrymme för försvararna att själva kunna anlita tekniskt sakkunniga för att granska och komplettera bevisningen. Möjligheterna för

[22] Se 9 kap. 1 § andra stycket och 3 § brottsbalken.
[23] Se 3 § lagen (1990:409) om skydd för företagshemligheter.
[24] Se 8 kap. 4 § och 36 kap. 5 § RB.
[25] Se Artikel 6.3 c) i Europakonventionen, och exempelvis NJA 2010 s. 122 och det särskilda yttrandet av justitierådet Stefan Lindskog.

offentliga försvarare att få ersättning av allmänna medel för anlitandet av tekniskt sakkunniga måste därför också ses över.

*Teknikneutralitet – uppgifternas skyddsvärde inte enbart beroende av teknisk miljö*

Sett i ett helhetsperspektiv måste påpekas att Advokatsamfundet finner det märkligt att uppgifter som finns i ett datorsystem skulle vara mer skyddsvärda än samma uppgifter när de förmedlas i ett elektroniskt meddelande via ett nät för elektronisk kommunikation. Samma uppgifter skulle även kunna vara inlåsta i ett fysiskt tillslutet förvaringsutrymme, som t.ex. ett kassaskåp. Därtill skulle uppgifterna kunna förekomma i ett slutet sammanhang där de obehörigen åtkoms genom anbringande av avlyssningsutrustning.

Teknikutvecklingen kännetecknas av en allt större teknikkonvergens, vilket medför att det blir svårare att skilja mellan när ett angrepp mot information ska anses utgöra brytande av post- eller telehemlighet, intrång i förvar, olovlig avlyssning eller dataintrång. Nät för elektronisk kommunikation omfattar till betydande delar datorer och datasystem. I förslaget framhålls också att moderna mobiltelefoner kan användas som datorer.[26] På detta sätt gör teknikutvecklingen det svårare att skilja mellan sådan elektronisk kommunikation som består i datorkommunikation och det slags kommunikation som omfattas av bestämmelsen om brytande av post- eller telehemlighet.[27]

Enligt Advokatsamfundet framstår det därför som naturligt att även brotten brytande av post- eller telehemlighet, intrång i förvar och olovlig avlyssning kompletteras med grovt brott på motsvarande sätt som den föreslagna brottsrubriceringen grovt dataintrång.

*Brottet dataintrång bör kompletteras med en bestämmelse om datastörning*

Advokatsamfundet anser även att det finns anledning att förändra den terminologi som i dag används. Begreppet ”dataintrång”, som det förekommer och beskrivs, antyder att någon obehörigen berett sig tillgång till uppgifter i ett datorsystem. Genom att föra in datavirus i systemet eller genom överbelastningsattacker störa eller hindra systemet eller dess användning, har inte gärningsmannen fått någon tillgång till systemet. Situationen kan snarare liknas vid att någon kastar en sten genom ett fönster. Därigenom har denne inte berett sig tillträde till lokalen innanför fönstret och således inte gjort sig skyldig till något olaga intrång. Däremot kan vederbörande ställas till svars för skadegörelse.

I såväl konventionen som direktivet används begreppen ”datastörning” eller ”systemstörning”. Med beaktande av detta anser Advokatsamfundet att den del av brottet ”dataintrång”, som består i att någon olovligen allvarligt stör eller hindrar användningen av uppgift i sådant system bör benämnas ”datastörning”, antingen direkt i 4 kap. 9 c § BrB

[26] SOU 2013:39 s. 67 f.
[27] Brottsrubriceringarna i 4 kap. BrB tillkom också under en tid då skillnaden mellan telenät och datorsystem var betydligt klarare.

eller i en ny bestämmelse (exempelvis genom en bestämmelse i 9 d §).[28] Därmed skulle större överensstämmelse också uppnås med både konventionen och direktivet.

## Synpunkter på de föreslagna ändringarna i lagen (2003:389) om elektronisk kommunikation

Lagen (2003:389) om elektronisk kommunikation (LEK) omfattar i huvudsak tillhandahållare av nät för elektronisk kommunikation eller elektroniska kommunikationstjänster. Endast ett fåtal paragrafer i lagen riktar sig även mot andra subjekt. Enligt Advokatsamfundet är det inte lämpligt att en speciallagstiftning som LEK även innehåller regler som vänder sig till enskilda individer. Om det nu ska införas regler i enlighet med förslaget om bevarandeföreläggande som kan riktas mot allmänheten, är det därför lämpligare att dessa regler finns i annan författning. Advokatsamfundet anser därför att bestämmelser om tystnadsplikt angående uppgift om bevarandeföreläggande lämpligen ska ges i 27 kap. RB i stället för som enligt betänkandets förslag i lagen (2003:389) om elektronisk kommunikation.

SVERIGES ADVOKATSAMFUND

Anne Ramberg

[28] SOU 2013:39 s. 88 ff., 91 ff. och 230 ff.