Stockholm den 15 februari 2018

R-2017/2282

Till Justitiedepartementet

Ju2017/08898/Å

Sveriges advokatsamfund har genom remiss den 6 december 2017 beretts tillfälle att avge yttrande över delbetänkandet Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89).

Advokatsamfundet avstyrker förslaget och hänvisar till de skäl som anförts i det särskilda yttrande som lämnats av Advokatsamfundets expert i utredningen (betänkandet s. 583-593).[1]

SVERIGES ADVOKATSAMFUND

Anne Ramberg/

genom Maria Billing

[1] Advokatsamfundet hänvisar även till sitt remissyttrande den 12 december 2017 över delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75) och de däri angivna remissyttrandena.

Särskilda yttranden

Särskilt yttrande av experten Anne Ramberg

Integritet - en rättighet som åtnjuter skydd

Genom Lissabonfördraget blev Europeiska unionens stadga om de grundläggande rättigheterna rättsligt bindande. Stadgan har samma rättsliga status som fördragen. I en gemensam förklaring anger medlemsstaterna att stadgan bekräftar de grundläggande rättigheter som garanteras av Europakonventionen (skyddet av den personliga integriteten och privatlivet regleras i artikel 8) och som följer av de konstitutionella traditioner som är gemensamma för medlemsstaterna. Det kan i det sammanhanget konstateras att den personliga integriteten och privatlivet dessutom åtnjuter skydd enligt artikel 12 i FN:s deklaration om de mänskliga rättigheterna och i FN:s konvention om medborgerliga och politiska rättigheter, Europarådets resolution från 1970, liksom i Europadomstolens praxis, EU-domstolens praxis samt i regeringsformen.

Att skyddet för den personliga integriteten och privatlivet upprätthålls är såväl ett enskilt intresse, som ett samhällsintresse. Övervakning genom hemliga tvångsmedel innebär ett integritetsintrång för den enskilde. Men, övervakning utgör samtidigt ett intrång i de rättsstatliga och demokratiska värden som den personliga integriteten ska skydda. Personlig integritet utgör ett villkor för att människor ska kunna utöva sina demokratiska rättigheter och därmed en förutsättning för det demokratiska samhället. Ett samhälle, där den personliga integriteten beskärs, riskerar att förlora sin demokratiska värdegrund, som bygger på allas fria och kritiska deltagande i debatten. Denna värdegrund förutsätter att människor i allmänhet inte upplever sig övervakade och registrerade. Skyddet är också en gräns för statens maktutövning och kan därför inte uppvägas av kontroll.

Inskränkningar i rättighetsskyddet

Det finns emellertid, under vissa i konventioner och lag angivna villkor, möjlighet att göra inskränkningar i rättighetsskyddet. En grundläggande förutsättning är att intrånget måste vara nödvändigt i ett demokratiskt samhälle. Ett behov måste föreligga och åtgärden måste förväntas bli effektiv. Därtill måste den vara proportionerlig i förhållande till syftet. Dessa krav följer av EU:s stadga om de grundläggande rättigheterna, Europakonventionen, regeringsformen och tydlig praxis från EU-domstolen och Europadomstolen för mänskliga rättigheter. Det innebär att en avvägning, mellan det befogade kravet på effektiv brottsbekämpning och upprätthållande av rättstrygghet för medborgaren, å den ena sidan och det lika befogade kravet på upprätthållandet av den enskildes rättssäkerhet och integritet å den andra, måste göras. Denna avvägning kan komma att utfalla olika vid skilda tidpunkter.

Hemliga tvångsmedel skulle ur ett brottsbekämpningsperspektiv kunna användas utan begränsning, inte bara vid brottsutredning, utan också i preventivt underrättelsesyfte. Det är lätt att se nyttoeffekter, såväl i det enskilda fallet, som generellt. Det är emellertid inte liktydigt med att det föreligger ett reellt behov av sådana åtgärder. Till detta anknyter problemet att effektiviteten är svår att definiera och mäta, något som i sin tur medför svårigheter i proportionalitetsavvägningen. En obegränsad användning av hemliga tvångsmedel är därför inte förenligt med grundläggande rättigheter skyddade i lag och konventioner.[1]

Krav på analys av behov, effektivitet och proportionalitet

Inledningsvis vill jag i detta sammanhang hänvisa till vad Advokatsamfundet tidigare anfört i yttrande rörande behovs-, effektivitets- och proportionalitetsprincipen vid hemlig dataavläsning och andra

[1] Se Advokatsamfundets remissyttrande den 30 oktober 2012 över betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44), den 18 maj 2009 över delbetänkandet *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen* (SOU 2009:1), samt den 30 januari 2007 över betänkandet *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98), liksom den kritik som Lagrådet anförde i sitt yttrande såväl den 13 maj 2014 (prop. 2013/14:237) som den 28 mars 2017 avseende fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen.

tvångsmedel, vilket alltjämt äger giltighet.[2] När det gäller frågan om det finns ett behov av att införa hemlig dataavläsning delar jag utredningens analys och slutsats att det, på de av de brottsbekämpande myndigheterna anförda skälen, föreligger ett behov som inte kan tillgodoses på annat sätt än genom hemlig dataavläsning. Till grund för denna slutsats lägger jag det faktum att lagstiftaren genom t.ex. inhämtningslagen, preventivlagen och i rättegångsbalken under vissa förutsättningar godtagit hemlig informationsinhämtning i underrättelseverksamhet och under förundersökning. Mycket av den information som med hjälp av nuvarande hemliga tvångsmedel tidigare kunnat inhämtas har dock av i utredningen redovisade skäl kommit att reduceras väsentligt. Således finns ett behov av att tillåta hemlig dataavläsning.

Jag delar likaså utredningens bedömning att hemlig dataavläsning skulle vara effektiv, i det enskilda fallet, då en sådan åtgärd skulle komma att användas. Det har emellertid från de brottsbekämpande myndigheternas sida samtidigt understrukits att hemlig dataavläsning i likhet med hemlig rumsavlyssning är tekniskt mycket komplicerad och mycket resurskrävande. Detta har uppgivits innebära att hemlig dataavläsning, i likhet med hemlig rumsavlyssning, endast skulle komma att användas i mycket begränsad utsträckning. I ljuset av det stora behov som uppges föreligga på grund av att en stor mängd information som tidigare kunde inhämtas med befintliga hemliga tvångsmedel, av en rad olika skäl, inte längre är tillgänglig, ifrågasätter jag om tvångsmedlet hemlig dataavläsning för närvarande skulle vara effektivt i strikt mening. Till detta kommer att risken finns att de personer och miljöer som skulle komma att bli föremål för hemlig dataavläsning snabbt skulle utveckla tekniker för att förhindra att informationsinhämtningen genom dataavläsning, på samma sätt som skett med traditionell avlyssning, skulle ge effektivt resultat. Detta sagt kan jag godta utredningens analys och slutsats när det gäller effektiviteten.

Jag delar dock inte utredningens analys och slutsatser när det gäller proportionalitetsavvägningen. Proportionalitetsprincipen är en erkänd rättsprincip i Sverige och i Europa. Den är lagfäst bland annat

[2] Se Advokatsamfundets remissyttrande den 30 september 2005 över promemorian *Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet* (Ds 2005:21). Se även Advokatsamfundets remissyttrande den 28 november 2005 över delbetänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38).

i regeringsformen, polislagen, rättegångsbalken, liksom i Europakonventionen och EU:s rättighetsstadga. Den följer därtill av Europadomstolens och numera EU-domstolens praxis. Principen äger generell giltighet vad gäller avvägningen mellan allmänna och enskilda intressen. Den betyder att statens metoder ska vara proportionerliga i förhållande till det berättigade ändamål som den avser att uppnå. I all synnerhet gäller detta i fråga om viktiga principer till skydd för den enskilde. När det allmänna intresset kolliderar med det grundläggande integritetsskyddet är statens handlingsutrymme särskilt begränsat. I en rättsstat ska den enskilde åtnjuta skydd mot statens maktutövning. Proportionalitetskravet innefattar en sådan begränsning. EU-domstolen bekräftade detta såväl i ogiltigförklarandet av datalagringsdirektivet som i den s.k. Tele2-domen.[3] Domstolen fastslog här att unionsrätten inte alltid tillåter intrång i privatlivet, ens om syftet i sig är godtagbart. Det krävs mer. Det krävs att åtgärden är nödvändig och att den vid en övergripande bedömning ryms inom statens handlingsutrymme. Min slutsats är därför att utredningens förslag om införande av hemlig dataavläsning inte är proportionerligt. Sammanfattningsvis finner jag utifrån principiella utgångspunkter inte utredningens förslag vara godtagbart.

Rättssäkerheten i teknikens våld

I den digitala utvecklingen har teknikimperativet blivit styrande. Det leder till en maktförskjutning från riksdagen till regeringen och rättstillämparen.[4] Vidden av integritetsintrånget kan nämligen utvidgas utan att lagstiftningen förändras. Det blir en s.k. tillämpningsglidning. Polisens basstationstömningar är ett sådant exempel. Detsamma gäller olika molntjänster. Teknikutvecklingen riskerar därmed att leda till att legalitetskravet åsidosätts. I detta hänseende är särskilt bestämmelserna i 17 och 19 §§ i den föreslagna lagen om hemlig dataavläsning av intresse.

[3] Se EU-domstolens avgörande den 8 april 2014 i de förenade målen C-293/12 och C-594/12 samt EU-domstolens dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15.
[4] Se Markus Naarttijärvi, *För din och andras säkerhet – Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, 2013, Skrifter från juridiska institutionen vid Umeå universitet, nr. 29.

Hemlig dataavläsning erbjuder i det närmaste obegränsade tekniska möjligheter att övervaka människor i realtid. De avgränsningar som utredningsförslaget anvisar utgör dock enligt min mening inte tillräckligt skydd varken för den enskildes rättssäkerhet eller integritet. De stora avgränsnings- och tillämpningsproblem som den föreslagna bestämmelsen i 5 § innebär erfordrar en vidare analys. Härutöver finns behov av ytterligare utredning. Ett sådant exempel är hur det överhuvudtaget ska vara praktiskt möjligt att kunna tillämpa begränsningarna i 4 § tredje stycket i den föreslagna lagen om hemlig dataavläsning.

Som historien under senare tid visat tillkommer lagstiftning inte sällan för ett ändamål, men utvidgas efter en tid till att omfatta andra ursprungligen inte avsedda ändamål. Exemplen är många. När ett tvångsmedel eller annan övervakning väl har införts, är det jämförelsevis enkelt att utvidga tillämpningsområdet allt eftersom. Förslaget att ge de brottsbekämpande myndigheterna tillgång till vad som inhämtas genom signalspaning är bara ett av många exempel. Detsamma gäller när hemlig tvångsmedelslagstiftning införs ”på prov” och efter en tid regelmässigt blir permanentad. Risken för ändamålsglidning är uppenbar och kontrollen riskerar till följd av den komplicerade tekniken att bli inget annat än en chimär.

Särskilt om Säkerhetspolisens särskilda uppdrag att förhindra brott

Intrånget i den personliga integriteten grundar sig vid underrättelseverksamhet inte på någon misstanke mot en enskild person, utan på riskbedömningar om brottslig verksamhet någon gång i framtiden. Tidigare krävdes att det fanns särskild anledning anta att en specifik person skulle kunna göra sig skyldig till de uppräknade brotten. Utgångspunkten nu är i stället nyttan som inhämtningen kan ha för den preventiva verksamheten. Inhämtningen är inte som tidigare kopplad till vissa brott utan till visst straffvärde. Enligt inhämtningslagen får uppgifterna hämtas in om de är av särskild vikt för att förebygga, förhindra, eller upptäcka brottslig verksamhet för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Sådana bedömningar riskerar, i en annan politisk kontext än den som vi lever i idag, att grundas på allt från etnicitet, religiös inriktning, sexuell läggning till politisk inriktning. Att i underrättelseverksamhet tillåta preven-

tiva metoder på det sätt som lagstiftningen numera medger är redan det ett avsteg från sedan lång tid erkända och tillämpade rättsstatliga principer. De brottsbekämpande myndigheternas (utöver Säkerhetspolisen) behov får i underrättelseverksamheten, anses tillgodosett genom befintlig lagstiftning och de förslag som nyligen presenterats i delbetänkandet av Utredningen om datalagring och EU-rätten, *Datalagring – brottsbekämpning och integritet* (SOU 2017:75). Att härutöver tillåta hemlig dataavläsning i underrättelsesyfte är därför enligt min mening inte proportionerligt när det gäller de brottsbekämpande myndigheterna i allmänhet. När det gäller Säkerhetspolisen kan enligt min mening dock en annan bedömning göras.

Terrorism och IT-attacker är exempel på reella hot mot vårt samhälle och den demokratiska rättsstaten. Säkerhetspolisen har härvidlag ett särskilt ansvar att förhindra att terrorattentat och andra allvarliga brott mot rikets säkerhet äger rum. Detta uppdrag skiljer sig på ett avgörande sätt från den öppna polisens. Säkerhetspolisens uppdrag tar därför till övervägande del sikte på underrättelseverksamhet i syfte att förhindra allvarliga brott. Detta framgår bland annat av användningen av preventiva tvångsmedel. Det är i princip endast Säkerhetspolisen som använder sig av denna möjlighet. Den öppna polisen har enligt uppgift från regeringens skrivelse till riksdagen endast vid ett fåtal tillfällen erhållit domstols tillstånd enligt preventivlagen.[5] Lagstiftaren har dock inte velat göra åtskillnad mellan Säkerhetspolisen och den öppna polisen, när det gäller möjligheterna till tvångsmedelsanvändning. Det tycker jag är olyckligt. Om hemlig dataavläsning överhuvudtaget ska kunna uppfylla kraven på proportionalitet måste, enligt min mening, tvångsmedlet exklusivt förbehållas Säkerhetspolisen vid misstanke om mycket allvarlig brottslighet som utgör hot mot rikets säkerhet och som har ett straffminimum eller förväntat straffvärde på fängelse fyra år eller mer.[6] Detta erfordrar dock ytterligare analys och utredning.

[5] Se Regeringens skrivelse 2016/17:69 *Redovisning av användningen av hemliga tvångsmedel under år 2015*.
[6] Se Advokatsamfundets remissyttrande den 30 oktober 2012 över betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) och det särskilda yttrande jag avgav i samband med den utredningen.

Materiella synpunkter på lagstiftningen

Jag vill utöver vad som anförts ovan, även framhålla några materiella synpunkter på den föreslagna lagstiftningen.

Hemlig dataavläsning är enligt förslaget ett eget hemligt tvångsmedel som ska beslutas av domstol och införas under en begränsad tid. Avsikten är dock att det inte ska gå längre, när det gäller den information som ska kunna inhämtas, än vad som är fallet med befintliga tvångsmedel. Hemlig dataavläsning är emellertid ett tvångsmedel som enligt min mening innebär särskilda integritetskränkningar för den enskilde och som i flera hänseenden går betydligt längre än övriga hemliga tvångsmedel. Mot denna bakgrund anser jag att detta tvångsmedel, om det införs, bör vara sekundärt till övriga tvångsmedel och tillstånd av domstol endast aktualiseras efter att det visat sig att ett redan beslutat tvångsmedel inte gett avsett resultat. Först i ett sådant skede bör hemlig dataavläsning kunna komma ifråga.

Eftersom det är av största vikt att hemlig dataavläsning används med stor restriktivitet och endast efter nogsamt uppställda rättsliga förutsättningar, anser jag även att den uppräkning av uppgiftstyper som föreslås kunna inhämtas genom hemlig dataavläsning i bestämmelsen i 2 §, måste förtydligas genom att det i de angivna punkterna uttryckligen hänvisas till de lagbestämmelser som reglerar dessa tvångsmedel. Det kan finnas risk för att det annars skapas alternativa rekvisit för tillämpning av dessa hemliga tvångsmedel och därmed även en utvidgning av tillämpningsområdet. Lagtekniskt innebär då förslaget att tillåtligheten och omfattningen av hemlig dataavläsning görs beroende av den s.k. inhämtningslagen, preventivlagen och rättegångsbalken. Genom att vidta ändringar i dessa lagar kommer tillämpningen av hemlig dataavläsning därigenom automatiskt att kunna utvidgas. Det är emellertid inte heller en lämplig ordning. Frågan bör ytterligare analyseras och lösningen måste tydligt framgå i lagen om hemlig dataavläsning.

När det gäller de särskilda begränsningar mot hemlig dataavläsning som föreslås i 11 §, undantas advokater från åtgärder enligt 2 §. Detta är en självklarhet och innebär ett upprätthållande av gällande rättsstatliga principer. Avlyssning eller övervakning ska aldrig kunna vidtas avseende elektronisk kommunikation som sker mellan en advokat och dennes klient. Det är i detta sammanhang viktigt att

understryka att den förtroliga kommunikationen mellan en advokat och en klient och advokatens i rättegångsbalken fastslagna tystnadsplikt är ett klientprivilegium och därmed finns för att i första hand skydda klientens intresse av sekretess (se NJA 2010 s. 122 och justitierådet Stefan Lindskogs särskilda yttrande i denna fråga).

De särskilda förbuden mot att använda hemlig dataavläsning mot bl.a. advokater har även direkt samband med de föreslagna bestämmelserna om beslagsförbud och avlyssningsförbud (21 och 22 §§). Beslagsförbudet i 27 kap. 2 § RB är direkt kopplat till frågeförbudet i 36 kap. 5 § RB. Det är därför viktigt att den rättsliga motiveringen för beslags- och avlyssningsförbudet även tillämpas i fråga om den allmänna förbudsbestämmelsen i 11 §.

Skyddet för advokatens verksamhet framgår även av bestämmelsen om tillträdestillstånd i 12 §. Det rör sig här om mycket långtgående åtgärder av integritetskränkande art som innebär möjlighet att kunna installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Enligt bestämmelsens andra punkt anges att ett tillträdestillstånd inte får avse en plats som stadigvarande används eller särskilt är avsedd att användas för verksamhet som bedrivs av advokater. Enligt min uppfattning är kravet på ”särskild anledning att anta” att informationssystemet kommer att finnas på platsen och att det inte räcker med ett allmänt antagande, utan att det måste krävas någon faktisk omständighet som med viss styrka talar för att det kommer att finnas där i vart fall någon gång under tillståndstiden, alltför vagt formulerat. Kravet bör skärpas ytterligare.

I sista stycket i 2 § framgår att det ska vara möjligt att hindra överförda meddelanden från att komma fram. Oaktat liknande reglering avseende hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § andra stycket rättegångsbalken, får detta enligt min mening anses vara ett långtgående komplement till övervakning som kommer att kunna utföras genom hemlig dataavläsning. Ett sådant förfarande ställer därför särskilda krav på förekomsten av effektiva rättsmedel för det fall ett sådant, felaktigt, myndighetsförfarande skulle föranleda en enskild ekonomisk eller personlig skada (se artikel 13 Europakonventionen).

De grundläggande förutsättningar som måste vara för handen för att hemlig dataavläsning ska kunna ske anges i 3 §. Dock framgår av denna bestämmelse att det är tillräckligt att göra en proportionalitetsprövning innan ett beslut fattas om hemlig dataavläsning.

Bestämmelsen bör enligt mitt förmenande kompletteras med krav på nödvändighet och effektivitet, dvs. även uppfylla den s.k. behovs- och ändamålsprincipen, för att detta tvångsmedel ska kunna aktualiseras.

I bestämmelsen i 6 § anges förutsättningarna för hemlig dataavläsning utanför en förundersökning. Även om kriteriet ”påtaglig risk” är detsamma som i preventivlagen, finns risk för att det i fråga om ett så pass långtgående tvångsmedel som dataavläsning utgör ett alltför oklart och vidsträckt kriterium. Enligt min uppfattning bör det krävas att det föreligger en ”uppenbar risk”. Vidare torde lokutionen ”en person” innebära att det inte uppställs något krav på kunskap om namnet på den person som kan komma i fråga för hemlig dataavläsning. Dock torde det även innebära att också annan person än den som misstänks för brott skulle kunna komma att omfattas av tvångsmedlet (t.ex. en familjemedlem som bor på annan adress än den misstänkte, jfr 12§). Detta förefaller vara att gå väl långt och bestämmelsen bör uttryckligen ta sikte på en viss person, även om det inte uppställs krav på misstanke om ett specifikt brott.

I bestämmelsen i 13 § anges att prövning av hemlig dataavläsning sker av rätten på ansökan av åklagare (dock med undantagsmöjligheten i de fall det kan anses vara ”fara i dröjsmål” enligt 14 §, då åklagaren interimistiskt får fatta beslut om hemlig dataavläsning och där rätten sedan skyndsamt ska pröva om det finns skäl för åtgärden). Eftersom detta överensstämmer med det tillståndssystem som finns för andra hemliga tvångsmedel, utöver inhämtningsfallen (10 §), är detta en lämplig ordning även för hemlig dataavläsning och innebär i förhållande till inhämtningsfallen en stärkt rättssäkerhet genom att Polismyndigheten eller Säkerhetspolisen inte själv får fatta beslut, utan att detta måste göras av en domstol. Dessutom tycks den föreslagna ordningen innebära att det ankommer på åklagare att i det enskilda fallet pröva om förutsättningar för hemlig dataavläsning föreligger, efter att den brottsbekämpande myndighet som vill utföra åtgärden har ansökt om det, vilket jag anser vara positivt. Härtill kommer att det i 29 § anges att SIN ska underrättas om en prövning har skett rörande hemlig dataavläsning, vilket också är en systemkonform och rättssäkerhetsfrämjande ordning.

Vidare konstaterar jag att den möjlighet som åklagare har att i brådskande fall besluta om hemlig dataavläsning enligt 14 §, ställer viktningen mellan effektiv brottsbekämpning och rättssäkerhet

ytterligare i fokus. Att ett så pass långtgående beslut som att besluta om hemlig dataavläsning ska ligga på åklagare, vilken sedermera kan komma att utgöra part i ett efterföljande brottmål, kan ifrågasättas utifrån rättssäkerhetsskäl. Detta gäller även om den föreslagna ordningen är densamma som gäller i fråga om hemlig avlyssning och övervakning av elektronisk kommunikation och hemlig kameraövervakning enligt 27 kap. 21 a § andra stycket RB, liksom enligt 6 a § preventivlagen. Det kan alltså ifrågasättas om ett så integritetskränkande tvångsmedel som hemlig dataavläsning innebär, ska kunna beslutas av en brottsbekämpande myndighet.[7] Att stadga att uppgifter som inhämtats på felaktig grund inte får användas i en efterföljande brottsutredning utgör inte ett tillräckligt skydd för den enskilde. Sammantaget anser jag att domstol alltid ska ansvara för prövning av hemlig dataavläsning. I vart fall bör kravet på att det ska föreligga risk för ”fördröjning av väsentlig betydelse” skärpas väsentligt.

Överlag anser jag att förslagen i betänkandet i flera avseenden innebär att alltför mycket inflytande över den hemliga dataavläsningen, såväl i fråga om form som innehåll, överlämnas till de brottsbekämpande myndigheterna.

I 18 § regleras teleoperatörernas medverkan i samband med verkställigheten av hemlig dataavläsning. Det föreslås ingen lagfäst skyldighet för operatörerna att medverka vid verkställigheten av den hemliga dataavläsningen, utan det är fråga om frivillig medverkan. Skrivningarna i betänkandet förutsätter dock att operatörerna kommer att samarbeta med de brottsbekämpande myndigheterna på frivillig grund. Detta är med beaktande av förbudet mot lagstiftning genom motiv direkt olämpligt. Det finns goda argument för såväl en medverkansskyldighet som en medverkansmöjlighet. Enligt min uppfattning måste det dock tydligt framgå om operatörernas medverkan ska bygga på en laglig skyldighet eller om den ska vara helt frivillig. Att såsom nu lagstifta kring en medverkansmöjlighet på frivillig grund, men underförstått uttala att operatörerna måste medverka för att den hemliga dataavläsningen ska kunna bli effektiv, är inte en god lagstiftningsordning. Vidare framgår det inte av bestämmelsen vilken form av bistånd som avses, även om det i för-

[7] Jfr Advokatsamfundets tidigare yttranden i denna fråga, bl.a. yttrandet över betänkandet *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98).

fattningskommentaren nämns vissa typer av åtgärder som operatörerna kan komma att tillfrågas om bistånd med. Det finns därför risk för att det kan uppstå praktiska problem i samband med förfrågningar från de verkställande myndigheterna om samverkan med teleoperatörerna.

I bestämmelsen i 20 § slås vissa aktsamhetskrav fast; olägenhet eller skada får inte förorsakas utöver vad som är ”absolut nödvändigt”. Vidare anges att ett tekniskt hjälpmedel som använts vid hemlig dataavläsning ska tas bort, avinstalleras eller göras obrukbart ”så snart det kan ske” efter att tiden för tillståndet gått ut eller tillståndet hävts. Jag anser att tidskravet bör skärpas ytterligare, till ”omedelbart” eller ”i direkt anslutning till”, för att minimera risken för att uppgifter inhämtas efter att tillstånd löpt ut eller hävts.