Stockholm den 28 november 2005

R-2005/1309

Till Justitiedepartementet

Ju2005/4823/Å

Sveriges advokatsamfund har genom remiss den 7 september 2005 beretts tillfälle att avge yttrande över delbetänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). Med anledning härav anför Advokatsamfundet följande.

Allmän bedömning

Med utgångspunkt från de intressen som Advokatsamfundet har att ta tillvara framstår de förslagna författningsändringarna som synnerligen långtgående – särskilt när den samlade effekten av föreslagna författningsändringar och förutskickade krav på att bevara trafikdata beaktas från integritets- och rättssäkerhetssynpunkt. Förslagen bör enligt Advokatsamfundets mening inte läggas till grund för lagstiftning utan en närmare genomlysning av vilka effekter som kan förväntas från integritets- och rättssäkerhetssynpunkt och hur en bättre balans kan uppnås mellan effektivitet och integritet, utan att befogade åtgärder för att utreda brott hindras. Härvid har samfundet beaktat att andra omfattande förslag nyligen lagts fram om en vidgad tvångsmedelsanvändning i IT-miljö – se Brott och brottsutredning i IT-miljö (Ds 2005:6). BRU har uttryckligen (s. 113) bortsett från dessa förslag, som bygger på konventionsåtagande.

Advokatsamfundet har i många sammanhang gett uttryck för sin oro för de ökade risker för integritetsintrång som kan bli konsekvensen av det stora antalet förslag till förändringar i det straffprocessuella regelverket som är aktuella. I direktiven till Integritetsskyddskommittén (Ju 2004:05, dir. 2004:51) anför regeringen att det kan finnas anledning att göra en samlad analys avseende förhållandet mellan den totala verkan av den *nuvarande* (vår kursivering) lagstiftningen om tvångsmedel och annan övervakning och skyddet för den personliga integriteten. Samfundet framhöll i sitt yttrande den 30 september 2005 över promemorian Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet (Ds 2005:21) att lagstiftning enligt förslagen i den promemorian inte borde

övervägas innan en redovisning av Integritetsskyddskommitténs analys förelåg. Samfundet har samma inställning i fråga om förslagen i detta betänkande.

Hemlig dataavläsning

Ett helt nytt tvångsmedel föreslås som innebär att en brottsutredande myndighet, efter tillstånd av rätten, ska få hacka sig in och plantera programvara för att ”avläsa” data, i hemlighet utan någon efterföljande underrättelse till den misstänkte. Myndigheten ska till och med, efter tillstånd av rätten, i hemlighet få installera hård- eller mjukvara för dataavläsningen på en plats som annars särskilt skyddas mot intrång; t.ex. en bostad. Till detta kommer att ”avläsningen” inte bara avser sådan information om användningen – s.k. trafikuppgifter – som avses vid beslut om teleövervakning. Även *innehållet* omfattas och tekniken gör en långtgående åtkomst och sortering möjlig när berörda informationssystem ska avläsas.

Utredningen för härvid inga närmare resonemang om de vitt skilda sätt på vilka informationssystem kan användas, t.ex. med inbyggda mikrofoner (alla bärbara datorer har numera mikrofon), kanske tillsammans med webbkamera. Tekniken och författningsförslaget gör det i princip möjligt att överföra och ”avläsa” informationen i realtid. Resultatet kan alltså bli att samtal avlyssnas när de pågår, om t.ex. IP-telefoni används, eller att det rum där informationssystemet finns kan betraktas som på film, om en webbkamera finns ansluten till den dator som i hemlighet ”avläses”. Har datorn inbyggd eller ansluten mikrofon torde den programvara som ”planteras” kunna instrueras att aktivera mikrofonen, om den inte redan är aktiverad. Samtal mellan personer i rum där informationssystem finns som är föremål för ”avläsning” skulle därmed kunna avlyssnas i realtid (buggning). Avgörande blir hur inplanterade tekniska hjälpmedel utformas och instrueras; ska t.ex. en redan aktiv mikrofon slås av?

Till detta kommer att omfattande informationsmängder i form av databaser eller handlingar kan ”avläsas” i ett system. Ett beslut om dataavläsning skall visserligen innehålla uppgift om ”det informationssystem tillståndet gäller”. Begreppet informationssystem brukar ges en synnerligen vid tolkning; se t.ex. ett rambeslut som gäller på området, där informationssystem definieras som en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas (Ds 2005:5 s. 17). Enligt författningskommentaren till 11 § förslaget till lag om hemlig dataavläsning ”finns det givetvis inget hinder mot att beslutet ger tillstånd till hemlig dataavläsning i flera informationssystem samtidigt” (s. 431). Lagtexten (se 5 §) och motiven synes alltså möjliggöra, efter beslut av rätten, att programvara för ”avläsningen” via nät installeras i hemlighet i en eller flera servrar hos bl.a. företag – t.ex. VOLVO eller SKF – om det finns särskild anledning att anta att en misstänkt har använt sig av eller kommer att använda sig av dem (synnerligen anledning krävs inte eftersom det inte är fråga om annans bostad). Efter särskilt tillstånd av rätten får även hemlig installation (utan företagets vetskap) ske på plats.

Trots att de beskrivna långtgående intrången synes kunna omfattas av författningsförslaget har BRU menat att hemlig dataavläsning bör få äga rum redan vid förundersökningar rörande dataintrång; dvs. brott som har en jämförelsevis låg straffskala och för vilka inte ens tele*övervakning* har fått äga rum förrän till följd av nyligen genomförda författningsändringar. Advokatsamfundet kan inte – om hemlig dataavläsning trots allt skulle införas som tvångsmedel – ansluta sig till att åtgärder som kan antas få längre gående verkningar från integritets- och rättssäkerhetssynpunkt än hemlig tele*avlyssning* skall kunna medges redan på den nivå där endast teleövervakning kan komma i fråga (en förundersökning om dataintrång o.l. kan inte grunda teleavlyssning).

Vid en prövning enligt den föreslagna lagen kvarstår visserligen en begränsning utifrån proportionalitet och det är möjligt att sätta upp särskilda villkor för ett tillstånd. Frågan är emellertid hur rätten och ett offentligt ombud – innan dataavläsningen inletts – ska kunna bilda sig en närmare uppfattning om förutsättningarna. Kan de brottsutredande myndigheterna t.ex. vara säkra på var den berörda datorn finns om åtgärderna sker via nät och att åtgärderna inte öppnar upp för intrång av andra? Finns informationssystemet möjligen helt eller delvis utomlands så att åtgärden skulle innebära ett intrång i det främmande rikets suveränitet och används någon teknisk svaghet så att även andra kan uppmärksammas på den och ta sig in i informationssystemet? Som ytterligare exempel på komplikationer kan nämnas att det offentliga ombudet – som enligt förslaget inte underrättas om att ett tekniskt hjälpmedel återtagits (se 13 §) – avses agera om återtagande inte sker (s. 391). Här behöver dessutom de processuella förutsättningarna belysas.

Slutligen kan en begränsning av lagens giltighet till fem år, med hänsyn till den snabba utvecklingen, knappast ses som provisorisk eftersom en översyn sannolikt hur som helst är nödvändig inom den tiden.

Sammanfattningsvis kvarstår så många frågor rörande tvångsmedlets utformning och verkningar från bl.a. integritets- och rättssäkerhetssynpunkt att förslaget inte utan ytterligare genomlysning bör läggas till grund för lagstiftning. Det bör härvid noga övervägas hur rätten och det offentliga ombudet skall kunna ta ställning till och i praktiken verka för en avgränsning av eventuella kommande beslut på området. De beskrivningar BRU ger synes i huvudsak ta sikte på effektivitetsvinster, utan närmare genomlysningar av möjliga begränsningar för att tillgodose rättssäkerheten och den enskildes personliga integritet.

Hemlig avlyssning och övervakning, m.m.

På motsvarande sätt har utredningen drivit frågan om effektivitet långt i sina förslag till vidgade möjligheter att avlyssna och övervaka telekommunikationer. Vad som på detta område helt synes förändra förutsättningarna för att bedöma och motverka allt för långt gående integritetsintrång är förslaget om att låta det brottsutredande organet själv – och först på verkställighetsstadiet – bestämma vilka teleadresser (tekniska hjälpmedel) som ett beslut om avlyssning eller övervakning ska omfatta. Det kan ofta stå klart att en viss person kan misstänkas för sådan brottslighet och under sådana omständigheter att förut-

sättningar för hemlig teleövervakning eller hemlig teleavlyssning i och för sig kan anses föreligga. Det återstår emellertid att avgränsa det intrång som åtgärden innebär.

Här kompliceras en bedömning av utredningens förslag av att – utöver att bestämningen av vad som ska få avlyssnas flyttas till verkställighetsstadiet - det föreslås en terminologisk justering. Denna terminologiska justering skulle enligt utredningen ha sin grund i utvecklingen på IT-området. I realiteten skulle en sådan ändring emellertid innebära en återgång till ett äldre, för IT-miljö knappast hållbart synsätt, nämligen att ett visst tekniskt hjälpmedel alltid skulle kunna pekas ut. Redan av utredningens egen beskrivning av vad tvångsmedelsanvändningen ska ta sikte på framgår emellertid att verkställigheten – trots den ändrade terminologin – avser ”identifierade enskilda telefonnummer eller e-postadresser” o.l. (se bl.a. s. 199); dvs. inte ett visst tekniskt hjälpmedel så som en viss dator eller telefonlur eller ett visst exemplar av en programvara t.ex. för IP-telefoni. Att verkställigheten avser vissa adresser via vilka kommunikation sker och inte viss telefonlur eller liknande blir särskilt tydligt när det beaktas att tvångsmedlet normalt verkställs hos en operatör, med avseende på viss eller vissa teleadresser, inte en viss telefonapparat, telefax eller liknande. Utredningens synes i denna del grunda sitt resonemang på att ingen precisering avses ske förrän på verkställighetsstadiet. Därmed krävs ingen notering i rättens beslut och det framstår som oklart hur det i efterhand ska kunna klarläggas vad verkställigheten har omfattat, om teleadresserna inte längre ska anges. Det bör härvid övervägas hur den parlamentariska kontrollen och JO:s granskning ska kunna verksamt motverka otillbörliga integritetsintrång.

Advokatsamfundets delar utredningens bedömning att nuvarande kontantkortshantering vållar betydande komplikationer. Utredningens förslag innebär dock att frågan om vilka teleadresser en verkställighet får omfatta undantas rättens prövning också i alla andra fall (fast telefoni m.m.), utan att några skäl för detta anges. I praktiken kan en mängd olika teleadresser aktualiseras, t.ex. till en tidningsredaktion, en advokatbyrå, en telefonkiosk eller liknande där åtgärder för verkställighet framstår som särskilt känsliga. En prövning av rätten bör kvarstå i vart fall för sådana teleadresser och för mobil telefoni o.l. där abonnenten finns noterad med namn för abonnemanget och i kataloger m.m. De oklarheter som berörts av utredningen rörande begreppets innebörd (s. 166) kan enkelt åtgärdas och utmönstringen av begreppet ”tele” skulle kunna ske på motsvarande sätt som för övriga begrepp så att endast termen ”adress” används i lagtexten.

Skulle berörda teleadresser i någon del få bestämmas först på verkställighetsstadiet bör de närmare förutsättningarna bestämmas tydligare än i förslaget och särskilda krav gälla, med möjlighet till prövning och överklagande i efterhand. För de allmänna ombuden torde uppdraget annars komma att framstå som mindre meningsfullt. I första hand bör alltså andra vägar än dem utredningen föreslagit prövas för att undgå hinder mot effektiva åtgärder för avlyssning och övervakning. Domstol och allmänt ombud torde inte få tillräcklig information om valen av övervakade eller avlyssnade adresser eller hjälpmedel flyttas till verkställighetsstadiet. Förslaget innebär ju att dessa förutsättningar skulle komma att klarläggs först senare, under verkställigheten av ett redan fattat tvångsmedelsbeslutet. I denna del behövs en närmare genomlysning av alternativa lösningar.

Sammanfattningsvis skulle det enligt Advokatsamfundets bedömning finnas risk för att domstolen och det allmänna ombudet närmast kommer att framstå som ett rundningsmärke, om den för frågan om integritetsintrång avgörande bedömningen av vilka teleadresser som ska få avlyssnas omvandlas till en verkställighetsfråga.

Vidare avstyrker samfundet förslaget att åklagare skall ges rätt att i brådskande fall fatta beslut om övervakning enligt förslaget till 27 kap. 19 § rättegångsbalken. Om behovet av att kunna fatta beslut snabbt är så stort som utredningen synes mena, kan det också finnas skäl att organisera domstolsverksamheten på sådant sätt att en domstolsprövning kan ske inom kort tid.

Övriga frågor

Förslagen leder sammantaget till en väsentligt ökad användning av hemliga tvångsmedel. Effekterna härav behöver som framgått genomlysas från integritets- och rättssäkerhetssynpunkt. Utredningen ger återkommande upplysningar om effektivitetsvinster och behoven av sådana, utan motsvarande genomgång rörande behoven av skydd för enskildas personliga integritet. En viktig del i detta sammanhang är vilka ekonomiska styrmedel som tas i bruk. Advokatsamfundet ansluter sig i denna del till Lars Trädgårds särskilda yttrande (s. 465) angående risken för överkonsumtion. Kanske skulle det rent av kunna bli fråga om en generell övergång från andra spaningsåtgärder till hemlig avlyssning, övervakning och dataavläsning. Denna risk bör bedömas tillsammans med förslaget att det först på verkställighetsstadiet avses bedömas vilka teleadresser och tekniska hjälpmedel som skall omfattas av åtgärden; dvs. att den brottsutredande myndigheten föreslås få egen kontroll även över detta led.

På samma sätt som Advokatsamfundet påpekat i tidigare sammanhang ges inte heller i detta betänkande några beskrivningar av vad som är tillåtet för ett företag eller en enskild som vill skydda sig om brottsliga angrepp. Problemen blir därmed alltmer accentuerade när legitima och behövliga skyddsåtgärder ska genomföras av enskilda utan att behöva riskera att själv göra sig skyldiga till brott till följd av att skyddet skulle kunna anses innefatta någon form av intrång eller annan otillåten åtgärd (jfr samfundets yttrande den 16 juni 2005 över Ds 2005:5 Angrepp mot informationssystem. Denna risk framträder särskilt tydligt om företag – när något oväntat inträffar i dess informationssystem – också skulle behöva beakta risker för att verktyg för hemlig dataavläsning kan ha installerats i hemlighet av en brottsutredande myndighet, som dessutom avses återta hjälpmedlet eller göra det obrukbart utan att skada i övrigt.

SVERIGES ADVOKATSAMFUND

Anne Ramberg