Stockholms universitet

2018-02-28 Dnr SU FV-1.1.3-4238-17

Regeringskansliet
(Justitiedepartementet)
103 33 Stockholm

Remiss: Hemlig dataavläsning- ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89)

Juridiska fakultetsnämnden vid Stockholms universitet har i sig inget att invända mot den problembild som Utredningen om hemlig dataavläsning (utredningen) beskriver i sitt delbetänkande. Fakultetsnämnden ser heller inga skäl att ifrågasätta att det föreligger ett behov av att införa ytterligare verktyg i den brottsbekämpande verksamheten, eller för den delen att hemlig dataavläsning skulle kunna utgöra ett effektivt bidrag i denna verksamhet. Fakultetsnämnden anser emellertid trots detta att det finns skäl till att vara kritisk till stora delar av förslaget. Fakultetsnämndens synpunkter anges i punktform i enlighet med utredningens sammanfattning av uppdraget (s 15 ff). Därtill lämnas synpunkter om lagförslagets regeltekniska och språkliga utformning.

1. Utredningen uppdrag var att ta reda på de brottsbekämpande myndigheternas behov av hemlig dataavläsning. Behovsanalysen som genomförts baseras i stor utsträckning på de aktuella myndigheternas egna redovisningar och flera myndigheter har redovisat typfall och exempel. Fakultetsnämnden ifrågasätter inte att myndigheterna korrekt beskriver upplevda behov. Emellertid saknas statistik och övergripande bild av behovets omfattning. De få kvantifieringar som anges, via jämförelser med faktiskt användning av andra tvångsmedel, indikerar snarast är behovet är begränsat (s. 283-284) men fakultetsnämnden menar att utredningen i detta avseende uppvisar sådana brister att den inte kan läggas till grund för ett beslut om att införa hemlig dataavläsning. Huruvida den aktuella kriminaliteten ökat, minskat eller har bytt skepnad går inte att fastslå genom anekdotiska exemplifieringar.

2. Behovsfrågan är nära kopplad till effektiviteten och fakultetsnämnden vill i detta sammanhang framhålla att avsaknaden av initial statistik (kontrolldata) om problemets omfattning, (se t.ex. s. 150-152) kommer att göra det omöjligt att utvärdera den tilltänkta lagens verkan och effektivitet. Lagförslaget brister därför också i relation till såväl EUs som OECDs rekommendationer om att ny

lagstiftning bör vara evidensbaserad och möjlig att utvärdera såväl ekonomiskt som kvalitativt. Utredningens egen slutsats att betänkandet ”motsvarar vad som ska finnas med i en kommittés konsekvensutredning vid regelgivning” i enlighet med Förordning (2007:1244) om konsekvensutredning vid regelgivning (s 488) är felaktig. I angivna förordning 4§ 1 st. 1 p. anges krav på att utreda kostnadsmässiga och *andra konsekvenser i den omfattning som behövs i det enskilda fallet* och dokumentera utredningen i en konsekvensutredning. Fakultetsnämndens mening är att det är oacceptabelt att föreslå en ny lag utan möjligheter att mäta det faktiska utfallet. Speciellt som utredningen själv anger att förslaget kommer att leda till ökade kostnader och i flera avseenden öka riskerna för enskildas personliga integritet.

3. Nyttan är av att införa ett tvångsmedel av aktuellt slag är nära kopplad till de tekniska möjligheterna. Utredningen konstaterar (s 240) att tekniker för att verkställa hemlig dataavläsning redan finns. Fakultetsnämnden instämmer och det handlar i stor utsträckning om att genom dataintrång placera mjukvara (”trojaner” i form av dataprogram) i annans egendom. Mjukvaran kan på flera sätt förändra den aktuella utrustningens funktionalitet, göra det möjligt att avläsa data och se hur utrustningen används.

   Fakultetsnämnden anser att den tekniska beskrivningen bör kompletteras och att utvecklingen ger en annan bild av den potentiella nyttan än den utredningen framför. Betydelsefullt är bland annat framväxten av Internet of Things (IoT ”sakernas internet”) som innebär att de mest skilda saker blir upp- och sammankopplade. Detta medför att data av olika ursprung och varierande typ kontinuerligt aggregeras, i telefoner, datorer, fordon, byggnader, och sensorer av otaliga slag. Data som kan kopplas till enskilda kan dock vara missvisande, p.g.a. att enskilda komponenter kan ha flera användare, för att de tidvis befunnit bortom ägaren kontroll, för att de är smittade med skadlig kod eller för att innehållet genom dataintrång manipulerats. Felkällorna i ett allt mer komplex IoT är oöverskådliga men gemensamt är att det i många fall inte går att utreda hur fel uppkommit (hur data aggregerats), eller ens upptäcka om informationen som härleds är felaktig, föråldrad eller måste kopplas ihop med ytterligare data för att bli rättvisande.[1] I fall där hundratals komponenter samverkar blir avsaknaden av spårbarhet påtaglig, konsekvenserna är outredda och metoder för kvalitetskontroll saknas eller är outvecklade.

   Analysen av kvalitativ effektivitet (s 286-290) återspeglar mot den bakgrunden en begränsad syn på vad uppgiftsinsamling av detta slag kan komma att innebära och

[1] Ett exempel är fordonsrelaterad data som autonomt genereras via textmeddelanden till brukarens telefon via bl.a. kalenderappar, geopositionering, koppling till brukarens fordon, m.m. Dessa meddelanden handlar om lämplig färdväg, tidsåtgång, trafiksituation m.m. rörande färd till den destination eller händelse (statistiskt eller på annat sätt identifierad) som systemet räknar med att brukaren ämnar sig till med hänsyn till klockslag, veckodag, tidigare rutiner m.m. Textmeddelandena kan i realtid och i efterhand avläsas i telefonen men är ibland felaktiga – brukaren valde vid vissa tillfällen en annan destination, använde att annat fordon, eller deltog inte i det identifierade mötet, men för att förstå det måste meddelandena kopplas ihop med ytterligare data, som kan vara otillgänglig. Exemplen är otaliga och utvecklingen är i sin linda.

fakultetsnämnden menar att utredningen i dessa avseenden är ofullständig. Frågor om vilka uppgiftstyper som ska behandlas och val av rimliga kvalitetskontroller är centrala komponenter att utreda då alla typer av nya IT-baserade system aktualiseras. Den förutsättningen gäller i hög grad även i detta fall. Till detta hör att § 2 i den föreslagna lagen om hemlig dataavläsning inte – som fakultetsnämnden uppfattat det – innehåller några egentliga begränsningar rörande de uppgiftstyper som får läsas av eller tas upp. Författningskommentaren till denna paragraf (s. 501) synes samtidigt felaktigt ange att ”[g]enom att punkterna i första stycket knyts samman av ordet *eller* ska klargöras att samtliga uppgiftstyper inte alltid får läsas av eller tas upp…” (Ordet eller saknas i förslaget till lagtext.)

I samband med detta ska tilläggas att fakultetsnämnden även känner oro över utformningen av 6 § som förslås innebära att tillstånd till hemlig dataavläsning kan komma att avse en organisation eller grupp. I kombination med att nära nog hälften av säkerhetspolisens i betänkandet redovisade typfall just handlar om utredning av misstankar mot att någon eller några i olika grupperingar (”personer i den autonoma miljön”, ”män i muslimsk ungdomsmiljö”, ”vit-maktmiljö”, ”slutet forum på internet”, etc.) väcks här frågan om de praktiska möjligheterna att hantera de mycket stora datamängder det kan komma att handla om. Politiska förskjutningar över tid är därtill ett reellt faktum och förslagets utformning synes öppna för en utveckling som innebär att mycket stora grupper kan komma att utgöra målgrupp.

4. Att tekniken att nyttja trojaner och liknande redan existerar och i vissa avseenden är lättillgänglig innebär att brukare med tillräckliga kunskaper relativt enkelt kan manipulera IT-baserade system. Detta kan ske på olika sätt, t.ex. genom att förändra innehållet i attackerade system och man kan tänka sig ett antal scenarion. Fakultetsnämnden vill inte här utveckla dessa i detalj men en risk som sammanhänger med en allmänt spridd kunskap om att de brottsbekämpande myndigheterna använder sig av denna teknik kan få till effekt att systemet avsiktligt kommer att överbelastas eller missbrukas. Detta kan exempelvis ske genom att komprometterande men felaktiga data i stor skala implementeras i personers eller gruppers utrustning. Förfarandet kan kombineras med att samordnade anonyma tips om förestående grova brott lämnas till myndigheterna. Systematiskt missbruk, men också enskilda händelser av detta slag kan inte bara komma att binda stora resurser. Det kan vara ytterligt komplicerade att utreda, och utredningarna kommer i sig att utgör avsevärda integritetsintrång för de oriktigt utpekade. Fakultetsnämnden menar att utredningen uppvisar brister avseende konsekvensanalyser. Frågan måste även ställas om i vilken utsträckning myndigheterna kan mobilisera teknisk kompetens.

5. Fakultetsnämnden vill därtill kommentera de bedömningar som görs i 3 § i Förslaget till lag (2019:000) om hemlig dataavläsning. Där lagfästs en proportionalitetsprincip med innebörd att ett tillstånd till hemlig dataavläsning får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse. Fakultetsnämnden anser att det är nödvändigt att proportionalitetsprincipen tydliggörs och lagfästs genom nämnda bestämmelse men att bestämmelsen behöver kompletteras till att omfatta också behovs- och

ändamålsprincipen. Behovet av en komplettering måste anses särskilt viktigt i syfte att om möjligt begränsa de synnerligen stora integritetsrisker som hemlig dataavläsning enligt utredningen innebär. En konsekvens av att bestämmelsen kompletteras till att också ställa krav på att det finns ett påtagligt behov av att använda hemlig dataavläsning och att en mindre ingripande åtgärd inte är tillräcklig (behovsprincipen) är att tvångsmedlet inte enbart blir ett komplement till befintliga tvångsmedel utan också blir sekundärt till övriga tvångsmedel. Enligt Fakultetsnämnden ligger en komplettering i nu nämnda avseende väl i linje med reglerna i regeringsformen, Europakonventionen och EU:s rättighetsstadga vad avser avvägningar hur intresset av en effektiv brottsbekämpning bör balanseras mot de integritetsrisker som identifieras.

Avslutningsvis vill fakultetsnämnden anmärka på den regeltekniska utformningen av lagförslaget om hemlig dataavläsning. De 31 paragraferna innehåller osedvanligt många, uppskattningsvis ca 90, interna och externa hänvisningar till andra stycken, andra paragrafer och till andra lagar. Skrivsättet innebär att det är komplicerat och tidskrävande att bedöma förslagets koherens och överblicka konsekvenserna i detalj.