Justitiedepartementet
Ju2017/08898/Å
103 33 Stockholm

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

Stiftelsen för Internetinfrastruktur (Internetstiftelsen) är en oberoende allmännyttig organisation som verkar för positiv utveckling av internet i Sverige. Vi ansvarar för internets svenska toppdomän .se, med registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret. Sedan september 2013 sköter Internetstiftelsen också drift och administration för toppdomänen .nu.

Internetstiftelsen har fått möjlighet att lämna remissvar och lämnar följande principiella synpunkter.

Utredningens sammansättning och avvägning
Sammansättningen består i stort sett endast av företrädare för brottsbekämpande myndigheter eller jurister inom rättsväsendet. Internetstiftelsen saknar företrädare för Datainspektionen som enligt Dataskyddsförordningen (GDPR) ska vara tillsynsansvarig myndighet för all dataskyddslagstiftning.

Det är enligt Internetstiftelsen centralt att frågan handlar om flera lovvärda intressen som delvis är oförenliga och därför måste vägas mot varandra. Om då företrädare från i huvudsak bara det ena intresset får stå för bedömningen riskerar den bli obalanserad.

Alltför starka polisiära befogenheter, utan tillräckligt skydd för den personliga integriteten, är inte förenligt med vad Internetstiftelsen definierar som ett fritt och demokratiskt samhälle, samtidigt som ett absolut skydd för individens personliga integritet skulle kunna leda till att de brottsbekämpande myndigheters verktyg blir trubbiga och verkningslösa. Internetstiftelsen förstår att det finns vissa användare som använder tjänster på internet som kan behöva spåras när de planerar att begå eller redan har begått allvarliga kriminella handlingar. Det betyder emellertid inte att det legitimerar alltför långtgående tvångsåtgärder. Därför är det viktigt att hitta en bra balans.

Det finns också händelser i historien som visar att en viss oro kan vara befogad. Ju större tekniska möjligheter samhället får att övervaka och kontrollera sina medborgare, desto större blir också risken för missbruk. Internetstiftelsen anser att det behövs en bättre utredning om riskerna för missbruk.

En principiellt viktig fråga är enligt Internetstiftelsen hur långt man kan gå för att skydda ett öppet och fritt demokratiskt samhälle med polisiära tvångs- och övervakningsåtgärder innan själva befogenheterna i sig innebär alltför stora ingrepp och riskerar att skada det öppna och fria demokratiska samhället.

Medborgarens personliga integritet

Internetstiftelsen vill att alla ska vilja, våga och kunna använda internet och vi är angelägna om att användningen av internet omgärdas med transparenta förfaranden och adekvata skyddsmekanismer samt att tvångsmedel som syftar till brottsbekämpning måste begränsas till vad som är nödvändigt och proportionerligt.

Utredningen drar slutsatsen att det är proportionerligt att införa regler om hemlig dataavläsning under förutsättning att reglerna balanserar de ökade integritetsriskerna och riskerna för informationssäkerheten som kan uppstå med hemlig dataavläsning. Enligt Internetstiftelsen har utredningen däremot inte tillräckligt utförligt förklarat hur förutsättningen ska uppfyllas, det vill säga **hur** balansen ska åstadkommas.

Man drar exempelvis ingen gräns mellan Säkerhetspolisen och den öppna polisen när det gäller möjligheterna till tvångsmedelsanvändning. Internetstiftelsen delar uppfattningen i utredningens expert, Anne Ramberg, särskilda yttrande i den frågan. Om hemlig dataavläsning ska kunna uppfylla kraven på proportionalitet måste tvångsmedlet förbehållas Säkerhetspolisen vid misstanke om mycket allvarlig brottslighet som utgör hot mot rikets säkerhet, förenade med högre straffsatser än vad som nu föreslås.

Enligt utredningen är hemlig dataavläsning en metod för brottsbekämpande myndigheter att med **någon form** av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som kan användas för kommunikation och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i den. Med den föreslagna metoden kan man alltså komma åt både uppgifter som i dag får hämtas in med nuvarande hemliga tvångsmedel och uppgifter som idag

inte får hämtas in med dagens hemliga tvångsmedel, till exempel uppgifter som finns lagrade i en dator eller telefon.

Utredningens förslag om hemlig dataavläsning sträcker sig inte bara till avlyssning av utrustning som datorer, mobiltelefoner och plattor. Förslagen omfattar även ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller likande tjänst, till exempel ett e-postkonto.

Vilka uppgifter som ska få läsas av de brottsbekämpande myndigheterna framgår av en punktlista på sidan 19 i betänkandet där punkt 6 de facto omfattar allt som finns lagrat i ett informationssystem. Något överraskande föreslår utredningen också att det inte bara handlar om att läsa av eller ta upp uppgifterna, utan att man också ska kunna hindra meddelanden från att komma fram. För Internetstiftelsen är det något oklart vad som avses och vilka konsekvenser det kan få.

De tvångsåtgärder som nu föreslås är enligt Internetstiftelsen mycket mer långtgående än vad som gäller idag eftersom polisen kommer kunna gå in i enskildas datorer eller annan utrustning. Det kan jämföras med en husrannsakan, med den skillnaden att den som utsätts för åtgärden inte har någon vetskap om att polisen är där.

Andra länders lagstiftning

Utredningen gör en mycket kortfattad internationell utblick som konstaterar att våra grannländer Danmark, Finland och Norge har liknande lagstiftning, utan att kunna göra någon närmare analys av utfall eller erfarenheter från detta med hänvisning till sekretess, och utan att kommentera att det i åtminstone Danmark och Norge krävs att det rör sig om brott med betydligt högre straffsatser – minst 6 respektive 10 år - än de minst 2 år som utredningen föreslår för den svenska lagstiftningen.

Motsvarande reglering i Tyskland prövades 2016 av den federala författningsdomstolen (BVerfG) som fann att lagstiftningen gjorde ett oproportionerligt intrång i den personliga integriteten och därmed måste ändras.[1]

De nya bestämmelserna föreslås ingå i en ny tillfällig lag som till att börja med ska gälla under fem år. Samma koncept har använts tidigare då nya möjligheter att använda tvångsmedel har införts i Sverige. Tillvägagångssättet kan enligt Internetstiftelsen ifrågasättas eftersom den

[1]http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2016/bvg16-019.html

riskerar att invagga medborgarna i någon sorts trygghet om att det hela ska omprövas efter en viss period. När provperioden är till ända är risken stor för att åtgärderna införs permanent då de flesta glömt att det var en tillfällig åtgärd och ingen, eller bara ett fåtal därmed protesterar.

Ett område där den här typen av åtgärder blir särskilt komplicerat är enligt Internetstiftelsen inom exempelvis journalistyrket. Källskydd, anonymitetsskydd eller tystnadsplikt som det också kallas, innebär att den som har tagit emot ett tips eller en uppgift inte får röja identiteten för den som vill vara anonym. Det är till och med straffbart för den som tagit emot en sådan anonym uppgift att avslöja källan. Källskyddet begränsar i vissa fall polisens möjligheter att använda tvångsmedel. Enligt utredningens förslag skulle reglerna om hemlig dataavläsning i olika hög grad ta hänsyn till källskyddet. När det gäller åtgärder som kan liknas vid hemlig rumsavlyssning föreslås det inte vara möjligt att avlyssna redaktioner. För åtgärder som mer är att likställa med avlyssning av elektronisk kommunikation skulle andra regler gälla. De reglerna innebär att polisen är skyldig att upphöra med avlyssningen om polisen vid avlyssning hör uppgifter som omfattas av källskydd. Å andra sidan betyder det enligt Internetstiftelsen att skadan i det fallet redan är skedd och källan får anses vara röjd.

Integritetskommitténs delbetänkande ”Hur står det till med den personliga integriteten?” innehöll en bilaga med en systematisk kunskapsöversikt över forskning kring frågan om på vilket sätt vi människor och vårt beteende påverkas av den accelererande digitala hanteringen av dennes uppgifter och privata sfär. Översikten togs fram av Lunds universitet och visar att det både internationellt och i Sverige finns förvånansvärt lite kunskap om vilken inverkan digital övervakning har på människans beteende och på hens uppfattning om världen och sig själv. Internetstiftelsen efterlyser fler insatser på forskningsområdet för att belysa detta.

Avlyssning och övervakning kan kränka medborgarnas rättigheter

All offentlig makt ska utövas med stöd i lag. När det gäller demokratins rätt att försvara sig mot odemokratiska rörelser är det särskilt viktigt att brottsbekämpande myndigheter inte överträder de regler som de folkvalda har ställt upp.

Det finns gråzoner när det föreligger hot mot rikets säkerhet, men i fredstid måste medborgarnas personliga integritet värnas mot övergrepp från statens sida. Den typ av övervakning som föreslås i utredningen kan enligt Internetstiftelsen stå i konflikt med de värden som beskrivs i författningsskyddsdelen av polisens uppdrag, och mot vad som är

acceptabelt enligt direktiv 2002/58, EU:s rättighetsstadga och Europakonventionen som beskriver viktiga principiella rättigheter för den personliga integriteten.

Avlyssning och övervakning är verktyg som vi historiskt sett förknippar med ofria samhällen och vi behöver även fortsättningsvis vara vaksamma mot eventuella regleringar och åtgärder som försämrar medborgarnas rättigheter. Resonemanget att det underlättar polisens arbete är måhända korrekt, men statens uppgift är inte att ensidigt underlätta polisens arbete genom att skapa inskränkningar i medborgerliga fri- och rättigheter som inte står i proportion till de integritetsrisker och integritetsintrång som förslaget om hemlig dataavläsning medför.

Användning av hackning och störning av utrustning är enligt Internetstiftelsen mycket långtgående åtgärder. Internetstiftelsen välkomnar därför också att användningen av sådana verktyg måste baseras på domstolsbeslut. Det är viktigt att både lagstiftaren och därefter domstolarna i sitt operativa arbete grundligt beaktar principerna om nödvändighet och proportionalitet.

Den svenska regeringen har som praxis att publicera årliga rapporter med statistik om brottsbekämpning. Internetstiftelsen uppmanar regeringen att lägga till information om både detta nya verktyg och andra införda tvångsåtgärder för att erbjuda en möjlighet att i efterhand analysera nyttoeffekter.

Utredningen föreslår att den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen om elektronisk kommunikation får bistå den verkställande myndigheten i samband med verkställighet av hemlig dataavläsning. Det borde enligt Internetstiftelsen inte vara operatören som vid varje enskilt tillfälle ska bestämma om de vill eller inte vill hjälpa till i brottsutredningen. Sådana beslut och överväganden bör inte överföras till privata företag, det är inte operatörernas roll och de är sannolikt inte heller rustade för att balansera mellan brottsbekämpande myndigheters behov och användarnas personliga integritet.

Tekniska överväganden

Enligt utredningen ska den verkställande myndigheten, om det är nödvändigt för att verkställighet ska kunna ske, få bryta eller kringgå skydd och utnyttja sårbarheter för att bereda sig tillgång till informationssystemet samt använda tekniska hjälpmedel i informationssystemet.

I utredningsdirektiven nämns hård- och mjukvara, mjukvarutrojaner vid sidan av fysisk placering av utrustning hos en misstänkt. Såvitt Internetstiftelsen kan bedöma handlar alltså dataavläsningen om att polisen kan kringgå krypteringen - inte bryta den - genom att bereda sig åtkomst till misstänktas datorer och telefoner innan kommunikationen hunnit bli krypterad. Frågan om hur man rent tekniskt ska kunna bereda sig tillträde utan att bibehålla kända sårbarheter som därmed blir öppna även för kriminella intressen har utredningen enligt Internetstiftelsen inte besvarat. Frågan är om det ens är möjligt.

Enligt Internetstiftelsen finns det en uppenbar risk för att de föreslagna åtgärderna bidrar till en osäkrare digitaliserad tillvaro för alla genom att säkerhetshål i de verktyg och tjänster vi använder inte täpps igen så snabbt som de skulle kunna. Med den tekniska säkerhetssidan följer också frågan om relationen till de företag som utvecklar tjänster och produkter.

Ta som exempel det amerikanska San Bernardinofallet där Apple vägrade att bistå FBI med att bryta sig in i en mobiltelefon som ägts av den skyldige vid en masskjutning.[2] FBI lyckades emellertid hacka sig in i telefonen på andra vägar, däremot fick Apple inte veta hur det gått till och utan den vetskapen kan det alltså finnas en säkerhetsbrist i Apples produkt som inte uppdateras och som kan användas vid flera, liknande ingrepp.

Ytterligare ett exempel är Wannacry, en skadlig kod som den 12 maj 2017 infekterade över 230 000 datorer i 150 länder. En av flera spridningsmetoder var nätfiskemeddelanden Attacken ansågs av Europol sakna motstycke. WannaCry ansågs använda sig av ett så kallat säkerhetshål som går under namnet Eternal Blue. Säkerhetshålet hade utvecklats av den amerikanska säkerhetstjänsten (NSA) för att kunna attackera datorer med Microsoft Windows som operativsystem. En säkerhetsuppdatering för att åtgärda felet utfärdades den 14 mars 2017, men saknade stöd för äldre versioner. Med anledning av den omfattande spridningen utfärdade Microsoft uppdateringar även för äldre system som de egentligen inte längre lämnar support för, till exempel Windows XP.

En fråga som Internetstiftelsen anser måste diskuteras är vilket ansvar de verkställande myndigheterna har gentemot de tjänsteutvecklare vars tjänster och produkter ingått i och medverkat vid den hemliga dataavlyssningen för att avhjälpa de brister som utnyttjats vid avlyssningen? Internetstiftelsen saknar i utredningen en fördjupad analys av tekniska osäkerheter och vilka följder detta kan få. En sådan utförligare utredning bör utföras av eller i samarbete med tekniska experter på

[2] https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute

området som kan bidra med väl avvägda insikter om vilka konsekvenser tvångsmedlet kan medföra ur ett tekniskt perspektiv.

Ändamålsglidning

I den frågan ställer sig Internetstiftelsen bakom en debattartikel i Dagens Juridik från 2016 där Stefan Larsson, docent i teknik och social förändring och doktor i rättssociologi vid Lunds universitets internetinstitut argumenterar för risker med ändamålsglidning, det vill säga att man först inför långtgående befogenheter för att bekämpa väldigt allvarlig brottslighet, något som sannolikt har stöd hos många och sedan successivt sänker ribban för vilken brottslighet som får bekämpas med sådana långtgående befogenheter, något som inte har stöd hos en bredare allmänhet.[3]

Nyttobedömning vs konsekvensbedömning

I utredningen har man enligt Internetstiftelsen lagt förhållandevis mycket kraft på att lyfta fram nyttoeffekten av hemlig dataavläsning trots att regeringens årliga redovisning till riksdagen avseende användningen av hemliga tvångsmedel inte ger stöd för att kryptering utgör något särskilt stort problem vid verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation. Den nyttobedömning som där görs, det vill säga vilken nytta de brottsbekämpande myndigheterna anser sig ha av tvångsmedlen, har enligt statistiken varit tämligen konstant över tid samtidigt som antalet tillstånd till hemlig avlyssning och övervakning ökat.[4]

Direktiven till utredningen ger inte utredningen i uppdrag att den ska utreda och analysera vilka konsekvenser förslag om hemlig dataavläsning, med de metoder som tas upp, får för informationssäkerheten rent principiellt, något som Internetstiftelsen anser vara en allvarlig brist. Det är vid bedömning om ett nytt tvångsmedel ska införskaffas minst lika viktigt som integritetsfrågorna att informationssäkerhetsfrågor vägs och balanseras mot effektivitets- och behovsfrågorna. En hög informationssäkerhetsnivå leder också till minskad risk för kränkning av den personliga integriteten hos användare av nätet och nätets tjänster.

Internetstiftelsen anser det bra att utredningen på eget initiativ behandlar den frågan och delar alltså utredningens uppfattning att risken för minskad informationssäkerhet inte enbart innebär en risk för den personliga integriteten utan också utgör en risk i sig, vilket innebär att informationssäkerhetsrisker som uppstår i samband med hemlig dataavläsning bör betraktas i ett vidare perspektiv än som enbart integritetsrisker. Internetstiftelsen anser därför att dessa

[3] http://www.dagensjuridik.se/2016/06/debatt-stefan-larsson-I
[4] http://www.regeringen.se/rattsdokument/skrivelse/2017/12/skr.-20171869/

informationssäkerhetsfrågor bör utredas vidare innan utredningens förslag kan värderas och besluts.

Tidigare utredningar

Beredningen för rättsväsendets utveckling (BRU) föreslog redan år 2005 att hemlig dataavläsning skulle införas som ett nytt tvångsmedel i svensk rätt men förslaget kritiserades hårt av många remissinstanser och ledde därmed inte till någon lagstiftning. I korthet handlade kritiken om att balansen mellan nyttan och graden av intrång inte var klarlagd. Internetstiftelsen anser inte att det klargörandet är tydligare i den nu aktuella utredningen.

Slutligen bör myndigheternas hackningsverksamhet uppmuntra privata enheter att engagera sig i aktiviteter som gäller deras egna produkter och tjänster i avsikt att undergräva digital säkerhet. Om en leverantör identifierar säkerhetsproblem i sina produkter, system eller nätverk är det deras ansvar att lösa detta problem kraftfullt och så snart som möjligt. Det borde inte finnas utrymme för att hålla systemet sårbart för någon hackning från vem det vara månde.

Internetstiftelsen kan föreställa sig att senare tids många förslag om ökade möjligheter och tvångsåtgärder grundar sig på en vilja att åstadkomma något gott, men den grundläggande principen bör alltid vara återhållsamhet och proportionalitet.

Vikten av kryptering

Kryptering är ett skydd för alla användare – inte bara ett sätt för kriminella att komma undan lagens långa arm. Hemligheten med kryptering är att man med hjälp av en hemlig parameter, eller nyckel, och beräkningar enligt en given regel, algoritm, förvränger uppgifter så att de inte går att tolka (krypto). Med hjälp av nyckeln och den omvända algoritmen kan uppgifterna återskapas till ursprunglig form (klartext). Kryptering måste erbjuda ett verkligt motstånd mot att någon utan kunskap om exempelvis krypteringsnyckeln kan forcera eller ”knäcka” kryptot. Främst för att tillgodose säkerhetsbehovet, men också för att stärka moralen hos användarna. Undermåliga krypteringslösningar medför en bristande tilltro till kommunikation över internet på ett säkert sätt liksom till möjligheten att lagra information på ett säkert sätt. En utveckling där brottsbekämpande myndigheter systematiskt ska kunna utnyttja sårbarheter eller installera vad som normalt betraktas som skadlig kod riskerar att undergräva förtroendet för samhällets digitalisering vilket enligt Internetstiftelsen är en långt större fråga än vad utredningen verkar förstå.

Sammanfattning

Om staten vidtar åtgärder för att inskränka den grundläggande rätten till ett privatliv ska det enligt Internetstiftelsen vara absolut nödvändigt, det ska inte finnas några mindre ingripande åtgärder som kan vidtas i stället och behovet och nyttan ska uppväga ingreppet i den personliga integriteten.

Att införa hemlig dataavläsning på det sätt och under de förhållanden som utredningen föreslår kan enligt Internetstiftelsen inte anses proportionerligt i förhållande till de risker för integritetsintrång som utredningens förslag innebär. Det kan enligt Internetstiftelsen också komma att påverka den allmänna inställningen till samhällets digitalisering och användningen av internet negativt.

En fråga som Internetstiftelsen inte heller anser vara tillräckligt belyst är vilken påverkan på rättssäkerheten utredningens förslag innebär. Hur lättvindigt kan till exempel de brottsbekämpande myndigheterna komma åt uppgifterna? Vilka är riskerna för missbruk? Vilka är riskerna för ändamålsglidning?

Utredningens förslag om hemlig dataavläsning saknar proportionalitet, är för omfattande och otydligt definierat. Internetstiftelsen avstyrker därför utredningens förslag i sin nuvarande utformning och anser att det krävs fördjupad analys på flera områden, både juridiskt och praktiskt innan lagstiftning om hemlig dataavläsning kan införas.

Stockholm den 8 mars

Stiftelsen för Internetinfrastruktur

Danny Aerts, vd