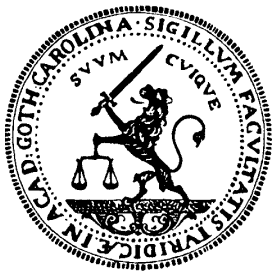


JURIDISKA FAKULTETEN
vid Lunds universitet

Johan Holmgren

Den allvetande staten

En utredning om den moderna teknikens inverkan på hemliga tvångsmedel samt diskussionen rörande integritet och rätten till anonymitet

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Professor Per Ole Träskman

Ämnesområde: Straff- och processrätt

Termin för examen: HT 2013

Innehåll

Summary

The conflict between the personal integrity and the judiciary's ability to use different kinds of secret coercive means is a classic question within the school of law. A question, which I believe has gotten too little attention, is how modern computer technology affects this discussion.

In my paper, I have therefore focused on three areas. First, I have researched how several secret coercive means, including covert wiretaps and surveillance of electronic communication, are affected by different implementations of the increasingly accessible encryption technology. In connection with this, I point out the difficulties of achieving the intended purpose of some legislation at all, for instance, the current criminalization of so-called file-sharing of copyrighted material.

Second of all, I have done a, depending on which aspect of encryption technology it concerns, more or less thorough review of both its current legality, but in some cases also which tendency one may find with the legislature and what the future holds.

For the third, I have investigated how the modern technology affect the relationship between the individuals' integrity and the States' ability for surveillance, also which intrinsic value the integrity concept should be considered protected. Here I have partially done a pervading examination of the view on secret coercive means in relation to individuals' integrity, which are expressed in a series of rulings from the European Court, but also those expressed in other legislatures, governmental investigations, and among individuals. I examine how these conclusions hold up when they are put against the abilities of modern technology, in combination with some historical events which I account for and put in the context of surveillance – integrity.

In my paper, I reach the conclusion that there exists great issues with the efficiency of current means of coercion when they are put against the encryption technology. But as I also conclude that the State, with the help of modern technology, has received immense possibilities for surveillance, I question the desirability of limiting the sphere of absolute anonymity and secure communication, which the encryption technology can provide. I also conclude that the view on the meaning of the concept of integrity and anonymity, which today is not only the dominant in the European Court and the Swedish legislature, probably doesn't allow for an acceptance of the legal situation concerning several aspects of encryption technology as it stands today; it's most likely that some type of legislation, which limit the possibilities for an effective use of some aspects of the encryption technology, will be introduced.

Sammanfattning

Konflikten mellan den personliga integriteten och rättsväsendets möjligheter att använda olika typer av hemliga tvångsmedel är en klassisk fråga inom juridiken. En fråga som jag anser har fått för lite uppmärksamhet är dock hur den moderna datortekniken påverkar den diskussionen.

I min uppsats har jag därför fokuserat på tre områden. För det första har jag undersökt hur flera hemliga tvångsmedel, bland annat hemlig telefonavlyssning och övervakning av elektronisk kommunikation, påverkas av olika implementeringar av den allt mer lättillgängliga krypteringstekniken. I samband med detta pekar jag på svårigheterna att över huvud taget uppnå det avsedda syftet med viss lagstiftning, exempelvis den nuvarande kriminaliseringen av s.k. fildelning av upphovsrättskyddat material.

För det andra har jag gjort en, beroende på vilken aspekt av krypteringstekniken det rör sig om, mer eller mindre grundlig genomgång både av dess nuvarande laglighet, men i vissa fall även vilken tendens man kan finnas hos lagstiftaren för hur framtiden ser ut.

För det tredje har jag undersökt hur den moderna tekniken påverkar förhållandet mellan enskildas integritet och statens möjligheter till övervakning, samt vilket inneboende värde integritetsbegreppet bör anses skydda. Jag har här dels gjort en omfattande undersökning av den syn på hemliga tvångsmedel i förhållande till enskildas integritet som kommer till uttryck i en serie avgöranden från Europadomstolen, men även den som kommer till utryck i annan lagstiftning, statliga utredningar, och hos enskilda. Jag undersöker hur hållbara dessa slutsatser är när de ställs mot den moderna teknikens möjligheter, i kombination med vissa historiska händelser som jag redogör för och sätter in i kontexten övervakning - integritet.

I min uppsats kommer jag fram till att det finns stora problem med effektiviteten hos nuvarande tvångsmedel när de ställs mot krypteringstekniken. Då jag även kommer fram till att staten genom den moderna tekniken fått oerhört mycket större möjligheter till övervakning, ifrågasätter jag dock det önskvärda i att helt inskränka den sfär av total anonymitet och säker kommunikation som krypteringstekniken kan tillhandahålla. Jag kommer dock även fram till att den syn på innebörden av begreppet integritet och anonymitet som idag är det dominerande inte bara hos Europadomstolen och den svenska lagstiftaren, troligen inte medger en acceptans av rättsläget rörande flera aspekter av krypteringstekniken som det ser ut idag, utan att det troligaste är att någon typ av lagstiftning som inskränker möjligheterna till ett effektivt användande av vissa aspekter av krypteringstekniken kommer att införas.

Förkortningar

EU – Europeiska unionen

TF – Tryckfrihetsförordningen

AES 256 – Advanced encryption standard 256 bitar

EKMR – Europeiska konventionen om skydd för de mänskliga rättigheterna

Prop. – Proposition

FRA – Försvarets radioanstalt

SIDA – Styrelsen för internationellt utvecklingssamarbete

RB – SFS 1942:740 Rättegångsbalk (1942:740)

TF – SFS 1949:105 Tryckfrihetsförordning (1949:105)

YGL – SFS 1991:1469 Yttrandefrihetsgrundlag (1991:1469)

PTS – Post och Telestyrelsen

NSA – National Security Agency

1 Inledning

1.1 Bakgrund

2011 skrev jag en kort uppsats rörande krypteringsteknikens påverkan på straffrätten. Hur agerar stater mot att allt mer av det människor gör och skapar flyttar över till den digitala sfären, samtidigt som det i teorin kan göras oåtkomligt från rättsväsendet med hjälp av kryptering? Hur hanterar man en situation där hårddiskar, telefonsamtal och e-post kan krypteras, och gamla beprövade spaningsmetoder som hemlig telefonavlyssning och husrannsakan därmed förlorar i värde, eller rentav blir helt obsoleta i de fall de behövs mest, som vid grov organiserad brottslighet?

När jag funderade över det här arbetet under 2013 så fick några av de här frågorna sina svar. Genom Edward Snowdens avslöjanden visade det sig att USA hade byggt upp ett oerhört stort övervakningssystem[1], och även skapat system för att komma runt och knäcka krypteringar, både genom att utnyttja bakdörrar i olika krypteringsprogram[2] samt genom att bygga in svagheter i datorer innan de ens levererats.[3] Dessutom kände inte ens president Obama till omfattningen av övervakningen.[4] I mitt föregående arbete hade jag sett hur stater försökt skapa en skyldighet att under straffhot uppge lösenord till krypterad information, parallellt med detta måste ett system för att komma åt informationen oavsett den misstänktes medverkan ha växt fram; en naturlig utveckling, då jag i min tidigare uppsats kom fram till att systemet med straffhot var både synnerligen ineffektivt och dessutom troligen stridande mot Europakonventionen.[5]

Det intressanta är dock vad det här säger om statens möjlighet att komma runt kryptering. Man hänvisas till att försöka utnyttja inbyggda svagheter i program, då information som krypterats med ett säkert program trots allt verkar helt skyddad från insyn. Den övervakning USA använder sig av, som inte verkar vara riktad mot genomsnittliga förbrytare, anser jag därför i sammanhanget vara av mindre betydelse.

Den stora frågan är istället vad som kommer att hända när i princip samtliga grova brottslingar, från narkotikahandlare till terrorister, använder sig av program för att kryptera sina E-postmeddelanden, hårddiskar och telefonsamtal. Vissa menar på att den andelen ökar exponentiellt.[6] Redan nu finns det program som är gratis och som har den funktionen, i flera fall finns det dessutom program som är "open source", vilket i korthet innebär att

[1] http://www.sydsvenskan.se/sverige/massavlyssning-avslojades--och-makthavarna-teg/
[2] http://www.gp.se/nyheter/varlden/1.2007113-de-knacker-din-kryptering
[3] http://www.sydsvenskan.se/Pages/ArticlePage.aspx?id=812870&epslanguage=sv
[4] http://www.svd.se/nyheter/utrikes/nsa-slar-tillbaka-obama-visste-inte_8662430.svd
[5] Se avsnitt 5.3
[6] Palfreyman, Brendan, Lessons from the Brittish and American approaches to compelled decryption, s. 347, tillgänglig via HeinOnline

källkoden kan granskas av kunniga användare, vilket både förhindrar "inbyggda bakdörrar" som myndigheterna kan ha begärt ska finnas med, samt gör det möjligt för en större grupp människor att hitta, och för programmerarna påtala, svagheter och säkerhetsluckor i programmet innan dessa hinner utnyttjas. Ibland kan detta vara komplicerat och dyrt, men det kan likväl genomföras.[7]

Krypteringstekniken i kombination med andra aspekter av den moderna tekniken, framförallt företeelsen ”Big data”, som jag också tar upp i min uppsats, väcker även andra frågor, som jag tror kommer leda till en omvärdering av synen på integritet kontra hemliga tvångsmedel. Med den här uppsatsen hoppas jag lägga en av de första byggstenarna till vad som troligen kommer att bli ett allt större forskningsfält, som vissa med god insyn menar på tidigare varit försummat.[8]

1.2 Syfte

I min uppsats kommer jag att sträva efter att skapa en helhetsbild över hur polisens klassiska tvångsmedel påverkas av krypteringstekniken, samt på vilket sätt lagstiftaren har agerat för att möta förändringen, för att därefter slutligen kritiskt granska om lagstiftarens förslag är rimliga ur ett integritetsperspektiv och hur de stämmer överens med Europadomstolens praxis. Jag kommer även att försöka kritiskt granska lagstiftarens förslag ur ett effektivitetsperspektiv, är lagstiftarens kamp för att ha möjlighet att komma åt all information möjlig att vinna? Och framförallt, bör den vinnas? Även här analyseras frågorna även ur ett teknikperspektiv.

1.3 Frågeställningar

– Vilken syn på integritet och anonymitet är allmänt rådande idag? Vilka konkurrerande teorier finns det på området? Vilken teori anser jag är rimlig att använda när det gäller tvångsmedel i förhållande till kryptering? Av vilka skäl?

– Vilken lösning föreslår jag på konflikten mellan krypteringstekniken och polisens nuvarande tvångsmedel?

– Hur ser rättsområdet ut idag vad gäller skyldigheten att uppge lösenordet till krypterad information? Vad har hänt på rättsområdet sedan jag skrev min tidigare uppsats "Kryptering, dekryptering och de mänskliga rättigheterna"[9]?

[7] http://arstechnica.com/security/2013/10/new-effort-to-fully-audit-truecrypt-raises-over-16000-in-a-few-short-weeks/
[8] Abrahamsson, Olle, SvJT 2009 sida 432
[9] http://www.lu.se/lup/publication/3046392

– Hur ser den rättsliga statusen för så kallade anonymitetstjänster[10] ut i dagsläget, och hur kommer lagstiftningen runt dessa troligen att se ut i framtiden?

Hemlig dataavläsning

Hemlig dataavläsning är ett långtgående tvångsmedel, som skulle kunna användas av brottsutredande myndigheter för att komma åt information som är krypterad. Det går ut på att antingen infektera en dator med ett virus för att polisen på så vis ska kunna "ta kontroll" över datorn och se allt som den används till, men även möjligheten att installera ett fysiskt objekt i exempelvis ett tangentbord som registrerar alla knapptryckningar är teoretiskt möjligt. Metoden kan på så vis komma förbi kryptering genom att lösenord som knappas in blir tillgängliga för polisen, eller att krypterad e-post och telefonsamtal avläses innan de krypteras och lämnar datorn eller telefonen.[11]

Detta väcker en mängd olika frågeställningar:

– Vad hände med förslaget?
– Är det förenligt med Europakonventionen?
– Bör det enligt mig vara förenligt med Europakonventionen om man ser på domstolens tidigare praxis?
– Vad säger man inom olika myndigheter om kryptering? Vad säger exempelvis åklagare och poliser om dagens svårigheter och möjligheterna till nya tvångsmedel?

1.4 Teori och metod

Det intresse som måste vägas mot nyttan av att använda ett tvångsmedel är givetvis den enskildes integritet. Ett krav på att varje enskild människa skall förses med ett chip som konstant rapporterar position ses troligtvis av de flesta som något som absolut inte bör förekomma. Att människor väljer att ha en mobiltelefon på sig som i princip gör detta är en sak, men de flesta är nog ense om att det ska vara möjligt att undgå ett sådant kontrollsystem om man vill. Det är helt enkelt för integritetskränkande för att det av staten ska kunna tvingas på den enskilde. En relevant fråga är då varför vi anser det, vilket inneboende värde har egentligen begreppet personlig integritet?

Jag har i mitt arbete därför försökt analysera mina frågeställningar ur ett integritetsteoretiskt perspektiv. Hur ser staten på den personliga integriteten? Hur stort skydd finns det i Europakonventionen, såsom den uttolkas av den Europeiska domstolen för de mänskliga rättigheterna? Hur ser andra författare på rätten till personlig integritet? Finns det en generationskonflikt i synen på "det fria anonyma internet", som något nytt

[10] Exempelvis http://bahnhof.se/priv/extra/anonym
[11] Se nedan avsnitt 5.2

mot vad som tidigare gällt för kommunikation, där telefoner direkt kunde avlyssnas men internet alltid setts som relativt anonymt?

Jag upplever att det saknas en djupare diskussion om vad integritet egentligen innebär när det kommer till hemliga tvångsmedel. Hoppar diskussionen förbi det enligt mig centrala, att skydda individen och grupper av individer från statens makt? Beroende på vilket synsätt man har på vad integritet innebär och vad den skyddar, kommer frågor om hur krypteringstekniken påverkar straffrätten att få helt olika svar. För att få klarhet i detta har jag vigt en del av min uppsats åt att granska olika synpunkter på vad den personliga integriteten innebär, och om den bör och anses innefatta en rätt till total anonymitet i förhållande till staten och andra. Jag har även låtit en teori om teknologins påverkan på de här frågorna genomsyra min uppsats. Detta gäller både teknikens möjliga användningsområden för den enskilde, i form av olika tekniker involverande kryptering, men även för staten i form av olika metoder för övervakning.

Utöver detta har jag använt mig av sedvanlig juridisk metod. Genom att tolka rättsfall, förarbeten och relevant litteratur har jag försökt att besvara mina frågeställningar.

För att underlätta för läsaren och skapa en röd tråd, för jag även en kontinuerlig diskussion genom uppsatsen.

1.5 Material

Bortsett från litteratur, juridiska artiklar, rättsfall och förarbeten har jag använt mig av ett direkt uttalande från en auktoritet inom krypteringsområdet om att det påstående jag gör om tekniken är korrekt. Detta för att kunna komma till snabba slutsatser runt de tekniska aspekterna, och istället fokusera på de juridiska frågor som väcks. Även i andra fall har jag fört en konversation med personer med kunskap om olika relevanta ämnen. Jag har dock försökt att i möjligaste mån illustrera tekniken och dess användning i tydliga exempel, så att dess betydelse för juridiken blir klar och tydlig.

Jag har i mitt arbete även använt mig av en stor mängd nyhetsartiklar som källor. Detta eftersom jag ansett det nödvändigt för att på ett bra sätt skapa en tydlig förståelse av hur den moderna tekniken påverkar och kan användas. Min uppfattning är att den frågan inte i tillräckligt hög grad kan åskådliggöras endast med hjälp av mer klassisk juridisk doktrin. Jag har här varit synnerligen noggrann med att kontrollera att den information som jag hänvisar till är korrekt.

1.6 Forskningsläge

Jag uppfattar det som att de ämnen jag tar upp i min uppsats i huvudsak är relativt nya. Som tidigare nämnts har den moderna teknikens påverkan inte

utretts i tillräckligt hög grad, och även integritetsfrågor verkar under en lång tid ha utretts endast schablonmässigt[12] Att skapa ett helhetsperspektiv som på djupet både ser till teknikens påverkan på tvångsmedel och på den personliga integriteten torde vara relativt nytt. En uppsats som berör krypteringsteknikens påverkan på polisens möjligheter till beslag kan dock nämnas.[13] Vad gäller den moderna teknikens påverkan på övervakning bör Neil M Richards ”The Dangers of Surveillance” nämnas, denna redogör jag för grundligt i uppsatsens avsnitt om integritet och anonymitet.

1.7 Disposition

I ett första avsnitt diskuteras krypteringsteknikens möjligheter, och hur dessa påverkar klassiska tvångsmedel och effektiviteten hos vissa lagar. Detta illustreras genom flera olika hypotetiska kriminalfall. Därefter går jag in på lagligheten hos de olika krypteringslösningarna.

I nästa stora avsnitt går jag igenom frågorna om integritet, anonymitet och den moderna teknikens påverkan på frågorna. Jag lyfter fram olika åsikter från personer inom både juridik, filosofi, och teknologi. I samma avsnitt lägger jag stort fokus på Europadomstolens syn på integritet i förhållande till hemliga tvångsmedel. Jag undersöker även här den syn på integritet och anonymitet som staten på olika sätt ger uttryck för. I detta avsnitt belyser jag även utifrån historiska händelser vissa faror med ett utbyggt system för övervakning.

I ett sista avsnitt går jag igenom de vägar runt kryptering som kan möjliggöras av tekniken och lagstiftaren. Därefter analyserar jag grundligt mina frågeställningar och besvarar dessa i min analys.

1.8 Avgränsningar

Många av de juridiska frågor som väcks är inte relevanta för mina frågeställningar, exempelvis är frågan om en inskränkning enligt artikel 8 skett "i enlighet med lag" förvisso omfattande och leder till många underfrågor, men då det mest handlar om hur mycket resurser staten vill lägga ned på att se till att lagstiftningen är tillräckligt tydlig och klar, är den inte relevant för mitt arbete. Att det räcker ”med lagstiftarens tre ord för att förvandla ett helt juridiskt bibliotek till makulatur"[14] har varit en ledstjärna för mitt val av frågeställningar.

Det som är intressant för min uppsats är istället de betydligt mer teoretiska frågorna om "nödvändig i ett demokratiskt samhälle", det däri inbyggda kravet på proportionalitet, teorin bakom personlig integritet, och hur

[12] Abrahamsson, Olle, SvJT 2009, s. 422
[13] Nicklasson, Larsa, m.fl, Problem vid beslagtagande av egendom, 2008
[14] Peczenik, Aleksander, Juridikens allmänna läror, SvJT 2005, s. 252

krypteringstekniken påverkar dessa frågor. Efterhand som jag skrivit mitt arbete har jag valt att lägga allt mer fokus på just teorin om integritet och anonymitet, då det under arbetets gång känts allt mer relevant för uppsatsen.

2 Kryptering

Kryptering är, i korthet, möjligheten att göra information oläslig för alla som inte har rätt lösenord. Det finns både svaga och starka krypteringar, jag kan exempelvis välja att kryptera det här dokumentet, som jag skriver i Microsoft Word 2003, med dess inbyggda krypteringsskydd, det skulle dock gå att knäcka den krypteringen relativt fort, både för en kunnig privatperson och för en brottsutredande myndighet.[15]

Om jag därför var orolig att någon tekniskt kunnig student skulle stjäla min uppsats och publicera den som sin egen, så skulle jag kunna välja att skapa en krypterad mapp med gratisprogrammet Truecrypt[16], som är ett program som kan använda sig av samma krypteringsalgoritmer som olika underrättelsetjänster använder sig av, AES 256, och sedan lägga min uppsats där. [17,18]

Förutsatt att jag valt ett lösenord som är långt och inte går att gissa enkelt, vare sig för en privatperson eller för en snabb dator som kan pröva vanliga lösenordskombinationer, kommer min information då, såvitt det är känt, att vara helt säker.

Om jag är ännu mer försiktig, och inte heller vill att studenter ska kunna titta igenom resten av min dator där jag sparat mina källhänvisningar, sökhistorik till uppsatsen eller liknande, kan jag helt enkelt välja att kryptera hela min dator istället. Detta medför att all information på datorn är omöjlig att få åtkomst till utan lösenordet.

I båda alternativen är informationen säker inte bara för en student som vill komma åt en uppsats, utan även för rättsväsendet. Oavsett om det är svensk polis eller den amerikanska underrättelsetjänsten som försöker komma åt innehållet i min dator, kommer försöken att misslyckas.

Detta beror, i korthet, på att det finns så oerhört många kombinationer av möjliga lösenord att det inte spelar någon roll hur kraftiga datorer man har till sitt förfogande, för överskådlig framtid är kryptering som utförts med Truecrypt eller liknande programvara helt omöjlig att forcera. Med Truecrypt tillkommer även möjligheten att skapa en s.k ”hidden partition” på datorn, denna är, enkelt uttryckt, krypterad information som i en myndighets ögon lika gärna skulle kunna vara en helt tom bit av hårddisken.[19, 20]

---

[15] http://lastbit.com/password-recovery-methods.asp#Guaranteed%20Recovery
[16] http://www.truecrypt.org/
[17] http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf sida 2
[18] https://www.iis.se/docs/lar-dig-kryptering.pdf 33-34
[19] http://www.truecrypt.org/docs/hidden-volume
[20] Palfreyman, Brendan, Lessons from the Brittish and American Approaches to compelled decryption, s. 355, not 64

Då det är ett uppsatsämne i sig att bevisa att kryptering är säker, väljer jag att inte gå djupare in på de tekniska aspekterna, utan väljer istället att av en expert på området få stöd för följande påstående, som jag sedan utgår ifrån genom hela min uppsats:

"Det är varken idag, eller inom överskådlig framtid, tekniskt möjligt att komma åt information som skyddats med stark kryptering såsom AES256. Detta under förutsättning att det inte finns svagheter i programmet som utför krypteringen, att man inte får tillgång till lösenordet, samt att detta inte är vare sig för kort eller för lätt att gissa."

Jag har fått detta påstående bekräftat[21] av Anne-Marie Eklund-Löwinder, säkerhetschef på stiftelsen .SE.[22] Stiftelsen ansvarar för administrationen och driften av det svenska toppdomänsystemet, det vill säga alla webbadresser som slutar på ”.se” eller ”.nu”.[23]

Krypteringstekniken möjliggör existensen av flera företeelser, vars effekter på polisens tvångsmedel den här uppsatsen bland annat försöker utreda. För att konkretisera de tekniska aspekterna har jag valt att diskutera dem, samt några av polisens klassiska tvångsmedel, i anknytning till tre tänkta kriminalfall.

Först diskuteras relevant tvångsmedel, därefter krypteringstekniken påverkan på detta, samt slutligen lagligheten av den krypteringstekniska lösningen i ett följande separat avsnitt.

2.1 Fiktivt kriminalfall, fildelaren Jimmy

Fildelaren Jimmy har valt att ladda ned den senaste skivan med Dimmu Borgir illegalt från nätet till sin hemdator. Detta är han dock förtegen om i kontakterna med vänner och bekanta, så några tips eller vittnesmål är inte aktuella i fallet. Frågan är nu vilka möjliga tvångsmedel respektive krypteringslösningar som aktualiseras i det här fallet, och hur de sistnämnda kan påverka rättsväsendets möjligheter att fälla Jimmy.

2.1.1 Informationsföreläggande

Det första polisen behöver för att få Jimmy fälld, är att koppla ihop den IP-adress de sett ladda ned albumet med den fysiska personen som står bakom adressen. För detta behöver de uppgifter från internetleverantören om vem som hade den aktuella adressen vid det aktuella tillfället. Då internetleverantörer idag är skyldiga att spara sådana uppgifter[24], och kan

[21] E-postkonversation med Anne-Marie Eklund-Löwinder den 17 november 2013
[22] https://www.iis.se/bloggare/anne-marie/
[23] https://www.iis.se/vad-vi-gor/
[24] Lag (2003:389) om elektronisk kommunikation 6 kap. 16a §

tvingas lämna ut dem även till företag och privatpersoner[25], så är detta ett effektivt sätt att få Jimmy fälld för brottet.

2.1.1.1 Krypteringsteknikens påverkan – Användandet av en VPN-tjänst

Krypteringstekniken kan här genom en VPN-tjänst, även kallad anonymiseringstjänst, användas för att skapa en krypterad länk mellan en vanlig hemdator och en server. Servern blir ett mellansteg mellan internet och hemdatorn. Om Jimmy använder sig av en sådan tjänst när han begår brottet, kommer polisen aldrig att se Jimmys IP-adress ladda ned albumet, istället kommer de se ett IP-nummer som tillhör anonymiseringstjänsten.[26]

Eftersom de flesta av dessa tjänster till skillnad mot internetleverantörer inte sparar någon information om vem som hade ett visst IP-nummer vid ett visst tillfälle[27], och informationen som skickas mellan Jimmys dator och anonymiseringstjänsten är krypterad, finns det inget sätt för polisen att ens hitta någon misstänkt, även om de redan misstänker Jimmy sedan tidigare och övervakar all datatrafik från hans dator. Man kan säga att spåren slutar redan där misstanken börjar om Jimmy använt sig av en sådan tjänst.[28] I bilaga två till uppsatsen har jag bland annat bifogat två bilder för att ytterligare förtydliga hur tekniken fungerar.

2.1.2 Husrannsakan samt beslag

Husrannsakan regleras i 28:1 RB. Det krävs att det finns anledning att anta att ett brott har begåtts på vilket fängelse kan följa för att husrannsakan skall få ske.

Beslag regleras bland annat i 27:1 RB. I första stycket klargörs att föremål som kan antas ha betydelse för utredning av brott kan tas i beslag. I tredje stycket framgår att tvångsmedel enligt kapitlet endast får beslutas om skälen för åtgärden uppväger de intrång eller men i övrigt som uppstår för den misstänkte.

Om Jimmy inte använt sig av en anonymiseringstjänst, så att polisen lyckas koppla brottet till hans internetabonnemang, är det givetvis en stor bevisteknisk fördel att kunna ta Jimmys dator i beslag, så att polisen tydligt kan se att albumet verkligen finns på datorn, att det ligger på Jimmys användarnamn, att det finns ett nedladdningsprogram installerat, etc. Det har nämligen inträffat att misstänkta försvarat sig med att ”datorn var kapad”, något som då får utredas [29]. I ett fall vid Lunds universitet där en doktorand i juridik misstänktes ha laddat ned barnpornografi från sin tjänstedator ledde

[25] Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk §53c p. 4
[26] Dnr: 08-12781, remissvar Post och Telestyrelsen, s. 2
[27] Exempelvis https://integrity.st/privacy/
[28] http://www.svt.se/nyheter/sverige/pedofil-utnyttjade-anonymitetstjanst
[29] http://www.svd.se/nyheter/inrikes/kapade-datorer-vanligare-i-rattsfall_8586848.svd

detta till en friande dom.[30, 31] Problematiken tas även upp i statliga utredningar.[32]

2.1.2.1 Krypteringsteknikens påverkan – Kryptering av hela eller delar av en dator

Precis som studenten som var orolig för att få sin uppsats stulen, kan Jimmy välja att kryptera hela eller delar av sin dator. Om han väljer att kryptera en del av datorn där han lägger det nedladdade albumet, är detta sedan omöjligt att komma åt, däremot riskerar han att polisens tekniker trots allt kan hitta annan information som kan knyta honom till brottet, såsom själva nedladdningsprogrammet, webbläsarhistorik som visar att han besökt den sida där albumet laddats ned, historik i datorn som visar att albumet spelats upp från datorn, eller liknande.

Om han däremot väljer att kryptera hela datorn, måste polisens tekniker ha lösenordet för att komma åt även den informationen. Datorn blir i praktiken värdelös för utredningen, eftersom det inte går att komma åt någon som helst information från den som kan styrka åtalet. Detta öppnar som sagt upp för argument från försvarets sida om att det i själva verket kan vara någon annan som begått brottet, antingen genom att ha hacka sig in i datorn eller genom att ha utnyttja ett öppet trådlöst nätverk[33], men även möjligheten till att det är någon annan med tillgång till en dator i hemnätverket som begått brottet kan i vissa fall bli aktuellt.[34]

2.2 Fiktivt kriminalfall, anläggaren Christian

Anläggaren Christian har beslutat sig för att sätta skräck i staten samt sin arbetsgivare med ett terrordåd, nämligen att anstifta flera andra anläggare att på ett snillrikt sätt bygga in svagheter i grunden till företagets senaste byggprojekt, ett stort hyreshus i centrala Stockholm, så att detta kommer att rasa när de välbärgade hyresgästerna väl flyttat in.

Då Christian inte uppgivit sin rätta identitet för de andra medlemmarna, utan bara anstiftat dem via telefon och e-post, måste polisen avlyssna kommunikationen både för att ha en chans att stoppa attentatet och för att få fast den verklige ledaren för terrorcellen och inte bara underhuggarna.

---

[30] http://www.dn.se/nyheter/sverige/man-friad-for-barnporr-i-datorn/
[31] http://www.expressen.se/kvp/doktoranden-med-barnporr-i-datorn-friad/
[32] SOU 2005:38 s. 364
[33] http://www.juridicum.su.se/iri/docs/Bevisfr%C3%A5gor_vid_upphovsr%C3%A4ttintr%C3%A5ng_genom_fildelning_m.m/
[34] http://dmca.cs.washington.edu/dmca_hotsec08.pdf

Frågan är nu vilka möjliga tvångsmedel respektive krypteringslösningar som aktualiseras i fallet, och hur de sistnämnda kan påverka rättsväsendets möjligheter att fälla Christian.

2.2.1 Hemlig avlyssning/övervakning av elektronisk information/signalspaning

Då det rör sig om en sluten terrorcell är det ett område där signalspaning kunde tänkas bli aktuellt. Så är dock inte fallet, då signalspaning inte får riktas mot kommunikation där både sändare och mottagare befinner sig i Sverige. Sådan kommunikation, om den oavsiktligt fångats upp, måste till och med omedelbart destrueras.[35] Om det istället hade rört sig om en terrorgruppering med kontakter i utlandet hade däremot lagen om signalspaning kanske kunnat aktualiseras, lika väl som den skulle kunna göra vid en enkel lagändring. Jag kommer därför trots allt gå igenom den närmre.

Försvarets radioanstalt (FRA) analyserar kommunikation på flera sätt. Man försöker dels fastställa vem som kommunicerar med vem, detta gör att man exempelvis kan fastslå hur en grupp är uppbyggd och personens sociala ställning däri utan att granska själva innehållet i kommunikationen.[36] När det kommer till innehållet i kommunikationen använder sig FRA av ett automatiserat system med sökbegrepp. Dessa består dels av nyckelord, men även andra omständigheter som var i världen meddelandet härrör ifrån.[37] Ett sätt att först komma gruppen på spåren vore alltså om deras kommunikation fastnade i den lista på ord och begrepp som FRA:s automatiserade system söker efter i den kommunikation som avlyssnas.

Hemlig avlyssning av elektronisk kommunikation innebär att elektroniska meddelanden som överförs mellan telefoner i hemlighet avlyssnas eller tas upp för återgivning av innehållet. Detta regleras i RB 27:18.

Hemlig övervakning av elektronisk kommunikation innebär bland annat att uppgifter kan inhämtas om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits, användandet regleras i RB 27:19.

Med hjälp av de två senare tvångsmedlen skulle polisen kunna få tillgång till kommunikationen mellan Christian och hans underhuggare, och avslöja både planen och Christans identitet, förutsatt att de har sådana misstankar mot dem att de kan använda sig av tvångsmedlen.

[35] Lag 2008:717 om signalspaning i försvarsunderättelseverksamhet 2 a§
[36] Klamberg, Mark, FRA:s signalspaning ur ett rättsligt perspektiv, SvJT 2009, s. 520
[37] Ibid. sida 529

2.2.1.1 Krypteringsteknikens påverkan – Användandet av krypterad kommunikation

Kryptering av E-post kan exempelvis göras i programmet PGP, som gör det möjligt att göra e-post oläslig för alla som inte har rätt lösenord för att öppna den. Om Christian, och de han skriver till, använder sig av sådana program kommer det vara mycket svårt[38] för polisen att ta del av innehållet i deras e-postkommunikation.[39]

Genom att utnyttja sig av en enkel krypteringstjänst för röstsamtal[40], kan han dessutom undvika att polisen får reda på någon som helst information genom att avlyssna eventuella samtal.[41]

Med övervakning av elektronisk kommunikation finns det dock en möjlighet för polisen att spåra positionen för den mobil som används. Detta försvåras dock givetvis avsevärt om ett oregistrerat kontantkort används som regelbundet byts ut. Anonyma kontantkort är det som regelmässigt används vid brottslig verksamhet.[42]

Genom att informationen är krypterad, ger den inga utslag när den genomsöks enligt FRA:s lista över ord och begrepp, detta betyder att oavsett om lagen om signalspaning skulle ändras så att även inhemsk kommunikation kan granskas, skulle den vara relativt verkningslös i det här fallet.

En teoretisk krypteringsteknisk lösning borde rimligen vara att kombinera användandet av en anonymiseringstjänst, användandet av ett program för att kryptera röstsamtal, samt att dessutom ringa samtalen med s.k internettelefoni[43] istället för via en telefon göra samtalen både omöjliga att avlyssna, samt dessutom omöjliga att positionsbestämma. Problematiken med kombinationen av internettelefoni och anonymitetstjänster har uppmärksammats av bland annat FBI.[44]

2.3 Fiktivt kriminalfall, droghandlerskan Maria

Droghandlerskan Maria har bestämt sig för att köpa in ett parti cannabis från en webbsida utomlands. Hon är medveten om samtliga tidigare nämnda krypteringslösningar för att skydda sin kommunikation, men vill även undvika risken för att banktransaktionerna kan knytas till hennes inköp; om

[38] SOU 2005:38 s. 363-364
[39] https://www.iis.se/lar-dig-mer/guider/digitalt-kallskydd-en-introduktion/skydda-kallan-e-post/
[40] Exempelvis https://itunes.apple.com/se/app/kryptos/id404884924?mt=8
[41] SOU 2005:38 s. 53
[42] Ibid. s 33-34
[43] Ibid. s. 53
[44] http://sakerhet.idg.se/2.1070/1.62051

paketet skulle fastna i tullen vill hon ha kvar möjligheten att hävda att det är feladresserat eller skickat till henne av någon illvillig person endast för att ge henne problem med rättsväsendet.

2.3.1 Lag om betalningsmedel

Marias rädsla är inte obefogad, då tillhandahållare av finansiella tjänster enligt Lag (2010:751) om betaltjänster har flera för situationen relevanta skyldigheter, som kan visa sig resultera i stark bevisning mot Maria vid en framtida rättegång. Här kan nämnas 3:14 som reglerar skyldigheten att lämna ut uppgifter relevanta för en brottsutredning, 3:8 som skapar en skyldighet att bevara sådana uppgifter i minst fem år, samt 3:15 som ger möjligheten att förbjuda tillhandahållaren av den finansiella tjänsten från att meddela den misstänkte om att uppgifterna om honom lämnats ut.

2.3.1.1 Krypteringsteknikens påverkan – Användandet av kryptovalutor

En lösning på problematiken är givetvis att Maria använder sig av kontanter som sänds via brev, men det är en relativt omständlig och långsam lösning, dessutom får brev öppnas under vissa omständigheter.[45] Ett effektivare sätt är då att använda Bitcoin, en så kallad kryptovaluta, som möjliggjorts av krypteringstekniken.

Utan att gå in alltför mycket på den relativt avancerade tekniken bakom, för den intresserade finns både en bra sammanställning[46] samt ett detaljerat paper[47], går tekniken ut på att ett bestämt antal bitcoin skapas i en viss takt, ett bitcoin är egentligen bara en krypterad bit information. Dessa får sedan ett värde av marknaden[48], och kan därför i teorin användas för handel.[49]

Det speciella med valutan är att det inte finns några banker eller stater som vare sig övervakar användandet eller garanterar dess värde. Den är helt decentraliserad, och en överföring mellan två personer är både anonym[50] och ospårbar[51].[52]

Maria kan således köpa valutan för riktiga pengar, och sedan via en datortransaktion omedelbart föra över den till mottagaren. Den enda transaktion som blir spårbar är således köpet av valutan. All den lagstiftning som införts om skyldighet att spara uppgifter om penningtransaktioner,

[45] SFS 1942:740 Rättegångsbalk (1942:740) 27:3
[46] bitcoin.org/en/how-it-works
[47] http://bitcoin.org/bitcoin.pdf
[48] http://www.gp.se/ekonomi/1.2161143-en-omstridd-valuta
[49] http://www.gp.se/ekonomi/1.2201671-det-har-ar-bitcoin
[50] Ibid.
[51] http://www.sydsvenskan.se/opinion/aktuella-fragor/det-vore-fullt-mojligt-for-politiken-att-framja-sadana-tekniker-istallet-for-a/
[52] http://www.di.se/artiklar/2011/7/24/droger-kan-bli-ny-natvalutas-fall/

bland annat för att förhindra terrorism, blir således i ett slag relativt verkningslös.

Givetvis är detta inte en möjlighet som den kriminella världen missat, relativt nyligen togs en webbsida ”The silk road” som utnyttjade sig både av anonymitetstjänsten TOR och valutan bitcoin i kombination ner, och ägaren greps.[53, 54] Man beslagtog då bitcoin till ett värde av över 33 miljoner dollar.[55]

Det bör poängteras att både i fallet där ägaren till sidan greps, och fallet där en av sidans större säljare greps, var det vanligt polisarbete som gav resultat, kombinerat med att personerna bakom tjänsterna gjorde misstag som ledde till att deras riktiga identiteter kunde avslöjas.[56, 57] För att garanterat hålla sig anonym via internet behöver flera faktorer nämligen vara uppfyllda. Att använda en anonymitetstjänst gör det förvisso omöjligt att få tag i personens identitet via IP-nummer, men om man skapar ett användarkonto på ett forum och vid registreringen använder sig av ett e-postkonto som man sedan använder även vid kontakt med exempelvis myndigheter, utsätter man sig för en risk att anonymitetsskyddet kan brytas igenom vid en samkörning av olika register.

Att så är fallet visade sig tydligt nyligen, dels då Expressen, med hjälp av Researchgruppen, utnyttjade sig av svagheter i diskussionstjänsten Disqus, för att koppla hundratals anonyma privatpersoner som kommenterat på bland annat Avpixlat, en sida starkt kopplad till Sverigedemokraterna, till sina riktiga identiteter för att sedermera hänga ut flera av dessa, något som resulterade i bland annat en uppsägning. [58, 59] Ett närmast identiskt händelseförlopp, bortsett från att myndigheter istället för enskilda fick tag i de relevanta uppgifterna, skedde när Ryanair via en domstol ville ha tag i identiteterna på anonyma anställda som kritiserade företaget på ett internetforum.[60]

Det är dock som sagt inte tekniken som brister, om de berörda personerna använt sig av en separat påhittad e-postadress, som Sveriges radio tipsat om[61] hade inte kopplingarna varit möjliga att göra i Expressenfallet. I Ryanairfallet var situationen mer komplicerad då en stat givetvis har tillgång till fler uppgiftskällor, men hade kommentatorerna skapat en separat e-

[53] http://swampland.time.com/2013/10/31/the-deep-web-has-washington-worried/
[54] http://www.theguardian.com/technology/2013/oct/15/silk-road-ross-ulbricht-alleged-mastermind
[55] http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website
[56] http://www.theguardian.com/technology/2013/oct/15/silk-road-ross-ulbricht-alleged-mastermind
[57] http://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/
[58] http://help.disqus.com/customer/portal/articles/1389598-statement2das
[59] http://www.di.se/artiklar/2013/12/12/chef-far-sparken-efter-inlagg-pa-avpixlat/
[60] http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5730621
[61]http://sverigesradio.se/sida/gruppsida.aspx?programid=4282&grupp=16907&artikel=5534626

postadress medan de var inloggade på en anonymitetstjänst, och aldrig vare sig loggat in på e-postadressen eller forumet utom från anonymitetststjänsten, och inte heller använt e-posten för personliga ärenden, hade det inte heller i det fallet varit möjligt att göra någon koppling, det hade då inte funnits någon IP-adress att begära ut förutom anonymitetstjänstens, vare sig hos e-postföretaget eller hos forumet.

Så länge bitcoin i sig är lagligt att använda, kommer sådana tjänster alltså troligen fortsätta att skapas, följaktligen återuppstod ”The silk road” tämligen omgående, och liknande sidor som sysslar med alltifrån vapenförsäljning till pengainsamling åt jihadgrupper existerar idag.[62]

[62] http://www.bbc.co.uk/news/technology-24842410

3 De krypteringstekniska lösningarnas laglighet

3.1 Kryptering av hela eller delar av en dator

Det finns i Sverige inte någon straffbestämmelse som kan användas mot någon som har krypterat sin dator och vägrar att uppge lösenordet till den. I bland annat England finns det däremot sådan lagstiftning, som jag tog upp i min tidigare uppsats.[63]

I avsnitt 5.2 går jag igenom den här typen av lagstiftning djupare.

3.2 Användandet av krypterad kommunikation samt kryptovalutor

Användandet av krypterad kommunikation är i dagsläget lagligt. Grupper som journalister kan givetvis ha ett extra intresse av att använda krypterad e-postväxling med tanke på källskyddet, användandet av krypterad e-post via exempelvis PGP ses som en lösning på bristande källskydd.[64] När Snowden tagit kontakt med The Guardian, fick inte journalisterna prata över telefon om vad som hade hänt. Istället fick de använda ett särskilt program för krypterad kommunikation.[65]

En lösning för krypterade samtal som också rekommenderas av journalistförbundet är open-source lösningen Redphone.[66] En större guide om olika tjänster gjordes av DN strax efter att riksdagen godkänt lagen om signalspaning.[67]

I dagsläget är också möjligheterna att använda bitcoin lagliga. Det är dock en relativt ny företeelse. Då den både kan användas som hjälpmedel vid grov organiserad brottslighet, och av storbanker generellt ses som ett hot mot deras affärsmodell[68], samt uppenbarligen gör en stor mängd lagstiftning ineffektiv, tror jag att det bara är en tidsfråga innan lagstiftaren kommer att sätta fokus på den. Helt nyligen tog Kina steg för att förbjuda användandet av valutan.[69]

[63] Holmgren, Johan Kryptering, dekryptering och de mänskliga rättigheterna, 2012
[64] Andersson, Sus, m.fl. Digitalt källskydd –en introduktion, 2012, s. 17+20
[65] http://www.sydsvenskan.se/kultur--nojen/storyn-med-stort-s--ett-besok-hos-the-guardian/
[66] https://www.iis.se/docs/sakrare-mobiltelefon.pdf
[67] http://www.dn.se/nyheter/politik/sa-forblir-du-anonym-pa-internet/
[68] http://www.va.se/helgintervjuer/helgintervjun-robin-teigland1-578149
[69] http://www.svt.se/nyheter/ekonomi/bitcoin-rasar-i-varde-efter-kinesisk-blockad

3.3 VPN-lösningar

Anonymitetstjänster är som framgått ovan ett oerhört kraftfullt verktyg för den som vill hålla sin identitet dold. Jag kommer därför att behandla och diskutera den nuvarande, och teoretiskt framtida, lagligheten av dessa mer ingående i mitt arbete.

3.3.1 Nuvarande lagenlighet

I dagsläget finns det inget klart förbud mot anonymitetstjänster, ett exempel på en sådan tjänst är internetleverantören Bahnhofs anonymitetstjänst ”Integrity VPN”.[70] En ytterligare intressant omständighet är att tjänster som TOR, som ger ett liknande resultat som en anonymiseringstjänst, i själva verket sponsrats av staten, via biståndsorganisationen SIDA. [71] Detta då anonyma kommunikationer ses som ett viktigt hjälpmedel för demokratiska krafter i diktaturer med repressiva övervakningssystem.[72] De kan dock som sagt givetvis lika väl användas för grov brottslighet[73], något man inte varit ovetande om från regeringens sida.[74] Att införa ett förbud mot en tjänst som TOR skulle därför vara ineffektivt, då själva syftet med tjänsten är att den skall fungera även i en repressiv diktatur som vill förhindra ett fritt informationsflöde. Till skillnad från kommersiella anonymitetstjänster, bygger TOR på ett decentraliserat system av enskilda frivilligas datorer som upprätthåller nätverket.[75]

År 2012 räknade man vid projektet Cybernormer vid Lunds universitet med att runt 700 000 svenskar använde någon form av anonymiseringstjänst.[76, 77]

Även om det inte finns någon lagstiftning som förbjuder den enskilde medborgaren att använda sig av en anonymiseringstjänst, kan det finnas andra förhållanden som leder till samma resultat. Ett sådant skulle vara att anonymiseringstjänster liksom internetoperatörer lyder under den skyldighet som införts genom datalagringsdirektivet[78], att bevara personuppgifter, och att tjänsterna, i den form de nu drivs där någon information ej sparas, i själva verket är olagliga.

[70] http://bahnhof.se/priv/extra/anonym
[71] https://www.torproject.org/about/sponsors.html.en
[72] http://www.sida.se/Svenska/Kontakta-oss/For-medier/Debattartiklar/Arkiv-2011/Debattartiklar-2011/Sa-skyddar-Sida-nataktivisterna/
[73] http://www.dn.se/nyheter/varlden/nathandelsplats-for-narkotika-stangd/
[74] http://www.dn.se/nyheter/sverige/nataktivister-ska-fa-svenskt-bistand/
[75] https://www.torproject.org/docs/faq.html.en#WhatIsTor
[76] http://www.dn.se/nyheter/sverige/allt-fler-svenskar-anonyma-pa-natet/
[77] http://sverigesradio.se/sida/artikel.aspx?programid=1646&artikel=5089677
[78] Direktiv (2006/24/EG) om lagring av trafikuppgifter

3.3.2 Anonymitetstjänster i förhållande till datalagringsdirektivet

I 6:16a Lag (2003:389) om elektronisk kommunikation fastställs att den som bedriver verksamhet som är anmälningspliktig enligt 2:1 samma lag är skyldig att lagra sådana uppgifter som avses i 20§ första stycket 1 och 3 som är "nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut."

I 6:20 samma lag fastslås i punkterna 1 och 3 att detta är uppgift om abonnemang (1) samt annan uppgift som angår ett särskilt elektroniskt meddelande (3).

I 2:1 fastslås att "Allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får endast tillhandahållas efter anmälan till den myndighet som regeringen bestämmer (tillsynsmyndigheten)". Denna myndighet är Post- och telestyrelsen (PTS).[79]

Frågan är alltså om anonymitetstjänster faller in under 2:1. När det kommer till frågan om hur man ser på VPN-nät hänvisar och upprepar Post- och telestyrelsen vad man sagt i förarbetena till lagen om elektronisk kommunikation.[80] I propositionen säger man att det är vanligt att virtuella privata nätverk används inom större organisationer, exempelvis för upprättande av säkra, krypterade, förbindelser vid uppkoppling av kunder eller anställda som befinner sig utanför organisationens nät. Detta kan ske över ett allmänt kommunikationsnät. Detta gör dock inte att den som tillhandahåller VPN-tjänsten är skyldig att särskilt anmäla denna verksamhet. Man konstaterar dock att den som tillhandahåller det allmänna kommunikationsnätet är anmälningspliktig för detta, under förutsättning att det tillhandahålls mot ersättning.[81]

I "Report from the commission to the council and the European parliament Evaluation report on the data retention directive (Directive 2006/24/EC)" konstaterar man kort att det finns ett allt vanligare utbud av tjänster som ligger utanför datalagringsdirektivets omfång. VPN-tjänster hos exempelvis universitet eller stora företag låter flera användare nå internet med samma IP-adress. Man konstaterar samtidigt att teknik för att koppla enskilda användare av tjänsten till adresser är under introducering.[82]

---

[79] Förordning (2003:396) om elektronisk kommunikation, 1:2

[80] Vilka tjänster och nät omfattas av LEK? En vägledning, Post och telestyrelsen, 2009, s. 47- 48

[81] Prop. 2002/03:110 s. 362

[82] Report from the commission to the council and the European parliament Evaluation report on the data retention directive (Directive 2006/24/EC) COM/2001/0225 final, s. 25

Den typ av VPN-tjänst som man förhöll sig till i propositionen och Europakommissionens rapport måste sägas vara väsensskild från de typer av tjänster som exempelvis Bahnhof driver. Trots detta bör man nog, som PTS hittills verkar ha gjort med tanke på att tjänsterna fortfarande bedrivs, tolka förarbetena som att VPN-tjänster faktiskt inte berörs av datalagringsskyldigheten i dagsläget.

Då rättsläget trots allt får sägas vara oklart och öppet för båda tolkningarna, har jag kontaktat en av juristerna på PTS, Peder Cristvall. Han bekräftade att PTS inte fattat något konkret beslut vare sig innebärande att anonymitetstjänster ska klassas som anmälningspliktig verksamhet och därmed lyda under datalagringsdirektivet, eller att de inte ska göra det. [83]

Ovanstående måste tolkas som att anonymitetstjänster dels är lagliga att använda för den enskilde medborgaren, dels dessutom i vart fall i nuläget är lagliga att driva i nuvarande form, dvs. utan att lagra trafikuppgifter.

Samtidigt är det tydligt att allt som krävs för att förändra situationen är att lagstiftaren utökar betydelsen av vad som menas med "Allmänt kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster" i § 20, alternativt att PTS fattar beslut om att anonymitetstjänster trots allt faller in under paragrafen.

Jag har därför valt att undersöka ämnet ännu ett steg djupare.

3.3.3 Framtida lagenlighet, tendenser hos lagstiftaren

Med ovanstående sagt är det inte klart att lagstiftaren är nöjd med utvecklingen, frågan om synen på anonymitetstjänster har bland annat kort berörts i följande fall:

I en skriftlig fråga till justitieminister Beatrice Ask berördes bland annat frågan om vilka åtgärder hon avsåg vidta "för att säkerställa operatörers möjlighet att tillhandahålla fungerande anonymiseringstjänster för internetanvändare".[84] Svaret blev att det inte var aktuellt med några åtgärder för att göra det möjligt att aldrig bli spårad på internet, då det är angeläget för bland annat brottsutredande myndigheter att få information om den typen av kommunikation.[85]

2009 ställdes en skriftlig fråga till Europakommissionen från en parlamentsledamot, om kommissionens syn på anonymiseringstjänster. Frågan rörde om kommissionen avsåg lägga förslag som förbjuder sådana tjänster inom vissa områden, om kommissionen ansåg att enskilda medlemsländer har rätt att förbjuda sådana tjänster, samt slutligen om

[83] Telefonkontakt den 23 december 2013, Peder Cristvall, PTS
[84] Skriftlig fråga 2007/08:507
[85] Svar på skriftlig fråga 2007/08:507

kommissionen ansåg att "rätten till elektronisk anonymitet är eller bör garanteras på EU-nivå".[86]

Kommissionens svar blev att de studerar anonymiseringstjänsternas inverkan på de rättsvårdande myndigheternas förmåga att skapa säkerhet för medborgarna, men att man inte planerade att lägga fram något förslag som förbjöd tjänsterna. Man konstaterar också att det är medlemsstaternas ansvar att värna om den inre säkerheten, och för det fall det skulle visa sig att tjänsterna begränsar möjligheten till detta kan de välja att lagstifta om tjänsterna, så länge de respekterar "den Europeiska konventionen om de mänskliga rättigheterna samt andra principer och garantier som rör de medborgerliga friheterna i Europa samt sina skyldigheter enligt fördragen."[87] I sådana fall måste åtgärderna vara väl underbyggda och stå i proportion till vad som är nödvändigt i ett demokratiskt samhälle. Man konstaterar även att det är viktigt att kunna lämna information anonymt för s.k. whistleblowers, och att det måste tas med i beräkningen när man överväger att lagstifta om tjänsterna.

Som svar på den sista frågeställningen säger man att medlemsstaterna kan anta åtgärder för att inskränka tillämpningsområdet för direktivet om privat och elektronisk kommunikation 2002/58/EG, som skyddar konfidentialiteten vid kommunikation, med hänvisning till exv. nationell säkerhet och brottsbekämpning.[87]

En annan intressant indikation på hur lagstiftaren ser på ett anonymt internet framgår i en rapport från kommissionen om internet och anonymitet[88] där man konstaterar att ”Det råder klar enighet om att verksamheten på internet inte kan undantas från de grundläggande rättsprinciper som gäller i andra sammanhang. Internet är inte ett anarkistiskt ghetto där samhällets regler inte gäller”.[89] Man konstaterar samtidigt att myndigheter inte ska ha större möjlighet att ”kontrollera potentiellt olagligt beteende på internet än i andra sammanhang utanför den digitala världen.”[89] Man fastslår som grundläggande princip att internet inte ska behandlas vare sig bättre eller sämre än äldre tekniker.[89] Det går dock som synes klart att utläsa att någon total möjlighet till anonymitet ej kan accepteras.

Något som är intressant är också att se hur lagstiftaren, i det här fallet näringslivsutskottet, resonerat vid införandet av Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG. Frågan om anonymitetstjänster lyftes nämligen vid olika tillfällen under arbetet med förslaget.

[86] Skriftlig fråga till Europakommissionen E-0897/09
[87] Svar på skriftlig fråga till Europakommissionen E-0897/09
[88] Rekommendation 3/97, Anonymitet på internet
[89] Ibid s. 6

I motion 2008/09: N9 (v) tar man upp frågan om "anonyma fildelningsnätverk", och hur dessa gör lagstiftningen ineffektiv.[90]

I en annan motion, 2008/09:N10 (mp), förs åsikten fram om att det finns en djupgående motsättning mellan jakten på fildelare och annan brottsbekämpning på internet. Man tror att effekterna av förslaget kommer att bli ett utökat användande av "anonymitetstjänster och s.k. darknets". Detta riskerar innebära att "terrorism, pornografibrott och narkotikabrott blir omöjliga att spåra."[91]

Utskottets ställningstagande till motionerna blir att dessa ej ska tillstyrkas. Man för dock inte fram några argument om vare sig effektivitet av lagstiftningen, eller risken att den leder till ett utökat användande av anonymitetstjänster, utan uppehåller sig vid andra argument, som att en fungerande upphovsrätt är nödvändig för att kulturskapande ska fortsätta.[92]

Senare i betänkandet diskuterar dock utskottet frågan om anonymisering av IP-adresser. Man anser dock inte att farhågorna är "beaktansvärda på ett sådant sätt att motionen bör föranleda någon åtgärd från riksdagens sida".[93]

Den kortfattade och närmast undflyende hanteringen av motionerna tror jag förstås bättre mot bakgrund av uttalanden i bilaga 4 som följer med utredningen, som är en nedskrivning av en offentlig utfrågning som hölls om införandet av lagstiftningen.

> "Låt mig avsluta med att kommentera påståendet att den här lagen skulle vara verkningslös, därför att det finns möjligheter att undgå ansvar genom så kallade anonymiseringstjänster. Så är det redan i dag när det gäller andra olagligheter på Internet. Vissa människor kommer alltid att försöka dölja sina spår, men det gör inte att vi struntar i att ha lagar och bestämmelser. Det vore helt orimligt i en demokratisk rättsstat.
> Denna reglering är dessutom utformad så att informationsförelägganden även kan riktas mot den som tillhandahåller en anonymiseringstjänst. Det vill säga, även den som har en anonymiseringstjänst kan bli föremål för ett föreläggande att informera om vem som döljer sig bakom olika IP-nummer."
> – *Statssekreterare Magnus Graner, Justitiedepartementet.*[94]

Med tanke på vad jag kommit fram till i det ovanstående, är det klart att statssekreteraren vid den här tiden inte insåg antingen vad en anonymitetstjänst var, eller under vilken reglering den skulle komma att lyda. Även om ett föreläggande kan riktas mot en anonymitetstjänst varken finns eller fanns det något tydligt krav på att de skulle spara någon information om "vem som döljer sig bakom olika IP-nummer" som kunde lämnas ut enligt föreläggandet. Statssekreterarens uttalande visar också på att han inte kunde ta till sig hur omfattande bruket av anonymiseringstjänster skulle bli. Jag får onekligen intrycket av att han ser

[90] Näringsutskottets betänkande 2008/09:NU11 Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG. s.26
[91] Ibid. s. 27
[92] Ibid.. s. 27-28
[93] Ibid. s. 33
[94] Ibid s.145

det som någon komplicerad svårtillgänglig lösning ingen vanlig medborgare kommer använda, därför är tekniken inte relevant i en lag för att bl.a. komma åt illegal fildelning, som ju var och är ett mängdbrott.

Den slutsatsen vinner stöd i ytterligare två citat:

> "Vad tror ni att det framöver kommer att krävas för insatser från oss politiker för att se till att vi klarar av den tekniska förändring som möjliggör den här typen av anonymitetstjänster"
> *–Tomas Eneroth (s).*[95]

> "Den andra frågan är viktig. Den berör teknikneutralitet. Jag vill återigen säga att jag är helt enig med vice ordföranden i näringsutskottet. Jag begriper mig inte heller på all denna teknik. Men det jag begriper mig på är att vi har en regel som säger att man har rätt att få betalt när man skapar ett verk. Och jag tycker att vi ska ha regler som gör det möjligt att följa upp det. Tekniken får så att säga komma i nästa steg. Och jag tycker att vi ska behålla det fokuset att försöka vara teknikneutrala så långt det är möjligt."
> *– Statssekreterare Magnus Graner, Justitiedepartementet.*[96]

Statssekreteraren avslöjar här öppet att han inte begriper sig på tekniken. Istället för att låta utreda frågan närmre har han valt att bara fokusera på ändamålet, att skydda de ekonomiska intressena inom upphovsrätten.

Utifrån ovanstående måste en rimlig slutsats rörande den rättsliga statusen för anonymitetstjänster vara att lagstiftaren helt enkelt inte förstått sig på dem, och endast därför underlåtit att lagstifta effektivt mot dem. De nämns över huvud taget inte i SOU 2007:76 som behandlar införandet av datalagringsdirektivet, istället visade sig samma mönster under debatten i riksdagen rörande genomförandet av direktivet. Argument om hur grova brottslingar skulle hitta vägar runt direktivet, om hur krypteringsprogram och öppna nätverk kunde påverka, togs upp[97] men ignorerades, istället fokuserade man på helt andra frågor.

Det verkar däremot otvetydigt vara så att lagstiftaren ser tjänsterna som ett hot mot bland annat intresset av att klara upp brott samt intresset av en välfungerande upphovsrätt.

Även om anonymitetstjänster därför både i dagsläget är lagliga att använda och driva, tror jag att det bara är en tidsfråga innan lagstiftarens uppmärksamhet vänds mot dem, på ett eller annat sätt. I SOU 2013:39 diskuteras en bevarandeskyldighet för olika uppgifter, och den lagstiftning som föreslås skulle vid en första anblick kunna tänkas användas för att komma åt information från anonymitetstjänster. Så är dock inte fallet, då det flera gånger betonas att skyldigheten bara gäller information som redan finns lagrad[98], och att ett föreläggande inte ska kunna användas för att

[95] Näringsutskottets betänkande 2008/09:NU11 Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG. s. 169
[96] Ibid s. 170
[97] Riksdagens protokoll 2010/11:73 p. 30
[98] SOU 2013:39 s. 257-259

begära att någon vid ett senare tillfälle skall spara uppgifter som då ej ännu existerar.[99] För en anonymiseringstjänst som inte sparar någon information är lagstiftningen alltså inte relevant.

[99] SOU 2013:39 s. 258-259

4 Integritet och anonymitet

Som jag tog upp i min inledning under teori, är frågan om integritet ytterst relevant i förhållande till användningen av hemliga tvångsmedel. Jag har därför i mitt arbete lagt stor vikt vid att se vilken syn på integritet staten har samt hur Europadomstolen ser på integritet kontra tvångsmedelsanvändning. Jag har slutligen även lyft fram andra åsikter rörande personlig integritet än de som förs fram från lagstiftaren och Europadomstolens sida, för att kunna analysera både nuvarande lagstiftning, dess samlade effekt samt föreslagen lagstiftning ur ett integritetsteoretiskt perspektiv. Jag undersöker här även åsikter rörande den hypotetiska rätten till anonymitet i förhållande till staten. När det kommer till andra författare har jag försökt göra ett urval där olika åsikter lyfts fram, både röster som i olika grad ställer sig kritiska eller positiva till övervakning har lyfts fram.

Anledningen till mitt stora fokus på Europadomstolens rättspraxis är att jag under min tid på juristlinjen fått det samlade intrycket av att Europadomstolen ofta blir den institution som dömer ut en åtgärd som en stat har gjort, de nationella domstolarna är inte lika snabba att göra detta. Det kan även tilläggas att processen att ändra eller tolka om Europakonventionen får anses vara betydligt svårare än att justera eller omtolka grundlagen.

I ett arbete som rör statens rätt på bekostnad av enskilda medborgare, är det enligt mig därför naturligt att främst undersöka den institution som är satt att skydda mot övertramp från statens sida i den typen av situationer.

Slutligen kan det onekligen ofta ligga i en stats intresse att låta lagstiftningen ligga rätt nära det Europadomstolen maximalt tillåter. Därför är ett klarläggande av domstolens praxis relevant även för att se vilken lagstiftning som kan tänkas introduceras på området i framtiden.

4.1 Statens syn på integritet och anonymitet

4.1.1 SOU 2005:38

Det är för mitt arbete givetvis relevant att se vilken syn på integritet staten har. Eftersom integritet är ett svårdefinierat begrepp och har olika betydelser i olika sammanhang, har jag till att börja med valt att belysa hur diskussionen runt integriteten gestaltat sig i SOU 2005:38, som bland annat rör tvångsmedlet hemlig dataavläsning, som jag kommer att redogöra för längre fram i min uppsats.

Man konstaterar här till att börja med att vid införandet av nya tvångsmedel, där syftet är att förbättra möjligheterna att bekämpa brott, är det ibland inte

möjligt att komma ifrån att integritetsintresset får stå tillbaka.[100]

Man konstaterar senare att det är en svår avvägning att göra mellan integritetsintresset och nödvändigheten av att myndigheterna har effektiva metoder när det gäller brottslighet. Man konstaterar dock att den kränkning den enskilde utsätts för ofta är liten i jämförelse med den som brottsoffret utsätts för.[101]

Ju allvarligare brottslighet det är frågan om, och desto mer problematisk den är för staten att utreda, desto mer tvingas samhället att tillåta i form av tvångsåtgärder för att bekämpa och utreda den. En kort men belysande mening som återkommer i utredningen är att "Det kan aldrig accepteras att brottsligheten tar överhanden och statsmakterna kapitulerar inför utvecklingen"[103]. Man anser också att "En utgångspunkt måste vara att ingen medborgare i varje situation kan hävda rätt till handlingsfrihet eller rätt att bli lämnad ifred"[102].[103]

Man hänvisar också till en statlig utredning från 1970-talet, där det bland annat uttalas att "en individ som lever i ett samhälle och sålunda ingår i en gemenskap med andra människor kan självfallet inte göra gällande något absolut anspråk på att få leva i fred för andra individer eller ostört av samhällets organ.”.[104]

Statens tolkning av Europakonventionen i SOU 2005:38

Man konstaterar att Europadomstolen funnit buggning, inspelning av telefonsamtal etc. som ingrepp i rätten till privatliv enligt artikel 8. Även om man kort nämner att det förutom att åtgärden måste vara ägnad för ett av de ändamål som nämns i artikeln och ha stöd i lag på ett så precist sätt att användningen blir förutsebar, och att det även krävs att åtgärden är nödvändig i ett demokratiskt samhälle vilket man menar betyder att den skall stå i rimlig proportion till det syfte den skall tillgodose kombinerat med att det skall finnas ett angeläget samhälleligt behov av den, så diskuterar man sedan inte detta närmre. Man diskuterar istället vad som krävs för att åtgärden skall klassas som laglig och förutsebar i tillräcklig grad, och konstaterar slutligen att "När teleavlyssning har ansetts utgöra en kränkning av artikel 8 har i de flesta fall bristande lagenlighet utgjort grunden för kränkningen"[105].[106]

[100] SOU 2005:38 s. 134
[101] Ibid. 135
[102] Ibid. 135-136
[103] Ibid. s. 135
[104] Ibid. s. 136
[105] Ibid s. 141
[106] Ibid. s. 140-141

4.1.2 Tryckfrihetsförordningen

Centralt för tryckfrihetsförordningen är att det existerar en rätt att vara anonym i kontakt med medier, då det råder ett efterforskningsförbud enligt TF 3:4 för myndigheter. Det råder dessutom enligt 3:3 TF tystnadsplikt för exv. journalister som fått ta del av en uppgift i förhållande till källan. Skyddet är dock inte oinskränkt, då vissa brott upphäver anonymitetsskyddet, exempelvis högförräderi i 7:3 TF 1 p.

Tryckfriheten är som bekant inte heller total, utöver brott som spioneri och krigsanstiftan regleras även brott som förtal, förolämpning och hets mot folkgrupp som tryckfrihetsbrott i 7:4 TF. I 8 kap. regleras ansvarighetskedjan för vem som är ansvarig för tryckfrihetsbrottet. En liknande reglering för yttranden på internet gäller enligt Yttrandefrihetsgrundlagen.[107] Enligt 1:9 YGL gäller detta dock under förutsättning att ett utgivningsbevis har meddelats samt att endast den som driver verksamheten kan ändra på innehållet i databasen.

Ett delvis likartat ansvarssystem gäller dock även för internetforum[108] trots att dessa inte skyddas av yttrandefrihetsgrundlagen, detta enligt Lag (1998:112) om ansvar för elektroniska anslagstavlor 1§ och 2§. Även här kan någon annan än upphovsmannen bli straffrättsligt ansvarig för begångna brott, detta enligt 5§ och 7§. Det rör sig här dock inte om någon ansvarighetskedja.

Det är tydligt att lagstiftaren här är beredd att sanktionera en viss anonymitet, men detta med förbehållet att det finns någon att straffa vid överträdelser. En absolut anonymitet står därför i stark kontrast även till den relativt generösa regleringen i ovan nämnda lagar, lagstiftaren vill trots allt ha möjligheten att kontrollera vilken typ av meddelanden som kan spridas, inte genom censur, men genom straffhot.

Å andra sidan vill man undvika en situation där staten likt under andra världskriget kan införa begränsningar av tryckfriheten[109] (Jmf förbudet att transportera periodiska skrifter via allmänna kommunikationsmedel)[110], i SOU 2006/96 menar man på att den demokratiska samhällsordningen kan hotas både av förhållanden inom och utom landet. I det sammanhanget nämns även kriget mot terrorismen.[111] Att tryckfriheten regleras i grundlagen och därmed inte enkelt kan inskränkas ser man som positivt för att förhindra detta, även om man anser att grundlagen i teorin relativt enkelt kan ändras. Den ”traditionellt breda uppslutningen kring tryck- och

[107] Axberger, Hans-Gunnar, Yttrandefrihetsgrundlagen, lagkommentar, inledande not, Karnov
[108] Prop.1997/98:15 sida 6
[109] SOU 2006/96 sida 227
[110] Modéer, Kjell, Juristernas nära förflutna, 2009, s. 247
[111] SOU 2006/96 s. 227

yttrandefriheten i Sverige" menar man dock skapar en tröskel för grundlagsförändringar.[112]

Det är då intressant att titta på den argumentation om signalspaningens påverkan på meddelarfriheten som förts. I proposition 2006/07:63 diskuterar man detta. Man kommer fram till att även om man inte riktar signalspaning mot dem som arbetar inom massmedia, kan man inte garantera att ett meddelande mellan en meddelare och en journalist inte avläses, något som medför att det anonymitetsskydd som garanteras genom journalistens tystnadsplikt genombrytes, dessutom kan en upptagning resultera i ett brott mot efterforskandeförbudet.[113]

Man anser att det ideala vore att inhämtning som berör massmedieområdet förbjöds, men detta är inte möjligt när denna är automatiserad, och av praktiska skäl är det inte heller möjligt att kräva att inhämtningen omedelbart skall avbrytas. Man kommer fram till att enda sättet att lösa problemet på är genom en föreskrift om att upptagningar som står i konflikt med tryckfrihetsförordningen och yttrandefrihetsgrundlagen omedelbart skall förstöras.[114]

Man delar inte tidningsutgivarnas bedömning att förslaget inte kan genomföras utan grundlagsreglering. Man anser att det är en stor skillnad på om information kan inhämtas, och om information inhämtas med syfte att bryta mot anonymitetsskyddet och efterforskningsförbudet, något som inte är aktuellt i fallet.[115]

Detta är en intressant detalj som återkommer på flera håll, både i denna och i andra utredningar; åsikten att blotta möjligheten till inhämtning av privat information inte utgör ett särskilt allvarligt integritetsintrång,[116] att utvidgade möjligheter till inhämtning av privat information i sig över huvud taget inte innebär en integritetskränkning[117] eller vad jag tolkar som att den stora integritetskränkningen ligger i om en fysisk person granskar kommunikation, och automatisk behandling av sådan information därmed inte är särskilt allvarligt ur integritetssynpunkt, har förts fram. [118,119]

[112] SOU 2006/96 s. 227-228
[113] Prop 2006/07:63 s. 105
[114] Ibid s. 105
[115] Ibid s. 106-107
[116] Prop. 2006/07:63 s. 88-89
[117] Dnr: 936-2013 Remissvar, Datainspektionen, 2013
[118] http://www.folkpartiet.se/politiker/ledamoter-av-riksdagen/johan-pehrson/debattartiklar/fra-och-signalspaning/
[119] Ds 2011:44, Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet s. 42-43

4.2 Andra författares syn på integritet

Jag kommer här att gå igenom ett antal andra författares syn på övervakning och integritet. Avslutningsvis berör jag även i ett eget avsnitt några av farorna med utbyggda övervakningssystem.

4.2.1 Integritetsskydd med eller utan förnuft

I en artikel i Svensk juristtidning går rättschefen Olle Abrahamsson ut och kommenterar debatten mellan förespråkare för integritet och förespråkare för övervakning.[120]

Han nämner att i den undersökning där han satt som ordförande, där man granskade integritetsbegränsande lagstiftning på en stor mängd områden, kom man fram till att lagstiftaren dels inte utredde integritetsaspekterna tillräckligt, dels bara schablonmässigt, ibland inte alls, prövade proportionaliteten hos åtgärderna.[121]

Han kommenterar dels att regeringen ställde sig bakom kommitténs slutsatser, dels att regeringen samtidigt som utredningen pågick bedrev ett intensivt reformarbete som försvagade integritetsskyddet, trots att flera remissinstanser ansåg att man först borde invänta kommitténs resultat.[122]

Han uppmärksammar också hur statsmakterna brukar hävda att insamlad information som bara finns latent tillgänglig i exempelvis dataregister inte inskränker rätten till privatlivet.[123] Han påpekar också att, den enligt honom felaktiga, åsikten att behandling av känslig information bara utgör en integritetskränkning om den görs felaktigt genomsyrar en stor del av lagstiftningen.[124]

Han kritiserar både dem som förespråkar mer övervakning och mer integritet, på olika grunder. De som förespråkar mer integritet anser han ofta tillhöra en liten intellektuell elit som tror sig företräda medborgarnas bästa, medan en stor del av befolkningen istället ställer sig positiva till bland annat kameraövervakning.[125] De som förespråkar övervakning anser han ofta för upp stereotypa argument som att den som har rent mjöl i påsen inte har något att förlora, ett resonemang han inte anser hållbart bland annat med hänvisning till Europakonventionen.[126]

Det som gör hans artikel intressant är den lösning på problemet som han förordar. Istället för att rikta in sig på frågan om hur övervakningen kan missbrukas, tittar han istället på medborgarnas uppfattning.

---

[120] Abrahamsson, Olle, Integritetsskydd med eller utan förnuft, SvJT 2009
[121] Ibid s. 421
[122] Ibid. s. 422
[123] Ibid s. 424-425
[124] Ibid s. 425
[125] Ibid s. 426
[126] Ibid s. 424

Han argumenterar nämligen utifrån att det viktiga är att medborgarna inte upplever att de lever i ett övervakningssamhälle, och kritiserar främst det nuvarande lagstiftningsarbetet ur det perspektivet. Integritetspåverkande lagstiftning skall vara så effektiv som möjligt, helst ännu effektivare än idag, utan att integritetskränkningsnivån ökar.[127] Hans lösning på problematiken är därför att minska bruket av övervakning som medborgare ser som integritetskränkande, exempelvis buggning, och kompensera med en ökning av t.ex. registeranvändning, något han menar mer än väl kompenserar för minskad tvångsmedelsanvändning.[128]

4.2.2 The Dangers Of Surveillance

Ett helt annat perspektiv på övervakning och integritet intas av Neil M Richards. I sin artikel ”The Dangers of Surveillance”, diskuterar han övervakning och vad som utgör faran med denna. Han anser att vi saknar förståelse för vad ”integritet” innebär, och varför den spelar någon roll, detta eftersom det inte varit aktuellt att ifrågasätta total övervakning, något som han anser hört till science fiction och misslyckade totalitära stater.[129]

Han börjar med att ta upp diktaturer som Kina som använder internet-aktivitet för att hitta dissidenter, under den arabiska våren försökte också de berörda staterna använda sig av data på sociala medier för att stävja revolterna.[130]

En intressant aspekt han tar upp är användandet av ”Big data”. Övervakning idag handlar inte om mappar i ett arkiv, utan om massiva mängder digital information om olika människor, som kan analyseras för att få fram nya slutsatser och resultat. Att tillsynes oändliga mängder data kan sammanställas och analyseras, i artikeln nämner han hur NSA byggt ett enormt datacenter för att avlyssna och lagra all internetkommunikation för analys[131], kommer att bli än mer kraftfullt i framtiden när man räknar med att alltifrån bilar till delar av hemmet kommer att anslutas till internet, på samma sätt som i princip alla idag bär runt på en gps-sändare via sin mobiltelefon.[132]

Ett exempel på användandet av ”Big data” som han tar upp är det amerikanska företag Target, som tar reda på vilka kunder som är gravida genom att analysera vilka andra produkter de köper. Nyblivna föräldrar är nämligen åtråvärda kunder då de dels köper mycket, och det dels är ett perfekt läge att knyta dem till sig när tidigare stabila köpvanor ändras. Genom att i det läget komma med riktad marknadsföring anser Target sig ha

[127] Abrahamsson, Olle, Integritetsskydd med eller utan förnuft, SvJT 2009 s. 429
[128] Ibid s. 430
[129] Richards, Neil, The Dangers of Surveillance, s. 1
[130] Ibid s. 6-7
[131] Ibid s. 2
[132] Ibid s. 8-10

en stor chans att knyta kunden till sig för lång framtid.[133] Det är med dagens teknik möjligt att följa enskilda individer på internet och konsekvent rikta skräddarsydda reklammeddelanden mot dem, så ofta att de troligen slutligen köper produkten.[134]

Google och liknande företag samlar uppgifter om köpvanor, intressen och internetanvändning, och andra företag skapar ännu mer detaljerad information om individer genom att kombinera olika typer av data, som de sedan säljer vidare exempelvis till företag som sysslar med bakgrundskontroller.[135] Läsplattor som Kindle sparar information ned till vilken sida man för tillfället läser.[136] Till detta kommer att staten har möjlighet att köpa, eller begära in, sådana uppgifter från privata aktörer.[137] Det finns idag en växande tendens där stater använder mjukvara för att profilera medborgare när det kommer till risk för kriminalitet.[138]

Han diskuterar därefter farorna med övervakning ur flera perspektiv.

Intellektuell integritet är idén om att nya idéer bäst utvecklas bortom allmänhetens blickar, att människor ska ha en rätt att fundera på saker på tider och platser de själva bestämmer, och att en meningsfull garanti om integritet är nödvändigt för att främja den typen av intellektuell frihet.[139]

Han baserar intellektuell integritet dels på att det är en del av själva kärnan i mänskliga rättigheter att medborgare har rätt till fria och ofjättrade tankar och åsikter, som minimum krävs då också rätten att läsa och tänka fritt, samt möjligheten att kommunicera privat med förtrogna.[140]

Dels baserar han det på att övervakning styr samhället till vad som är alldagligt och tråkigt. Om vi övervakas när vi surfar, läser och kommunicerar, vill vi inte göra saker som andra finner avvikande. Övervakning hotar därför intellektuell mångfald och ”excentrisk individualitet”. Detta menar han vinner stöd i flera undersökningar.[141]

Ett annat perspektiv är maktperspektivet. Information som samlats in kan användas för andra saker än vad den var tänkt för, vare sig det är utpressning eller diskrediterande av motståndare genom att avslöja pinsamma hemligheter. Han tar upp fallet med hur Martin Luther King behandlades av FBI: då man var orolig över att han var ett ”threat to public order” avlyssnade man hans telefon för att försöka få fram information som man kunde utpressa honom med. Man avlyssnade bortsett från hans telefon

[133] Richards, Neil, The Dangers of Surveillance s. 9
[134] Ibid s. 32
[135] Ibid s. 34
[136] Ibid, s. 8
[137] Ibid s. 2, 11
[138] Ibid s. 34
[139] Ibid s. 18
[140] Ibid, s. 18
[141] Ibid s. 21-23

även medarbetares, hotell etc.[142]

Han tar upp hur situationen hade sett ut idag, då även e-post, internetvanor, läsvanor etc. kan övervakas. Systemkritikern skulle kunna utpressas, eller diskrediteras för att statuera exempel. Kanske han har haft en otrohetsaffär, har någon medicinsk åkomma, besöker pinsamma hemsidor, etc. Att de forna kommunistarkiven används till sådant menar han än idag vara en risk.[143] Moamar Gaddafi försökte exempelvis samla in internet- och telefonkommunikation för senare undersökning med hjälp av västerländska teknikföretag. Med den tekniken lyckades Libyen få reda på saker om dissidenter som gjorde att de kunde tysta dem.[144]

Övervakning upptäcker ofta brott som ligger bortom eller utanför det ursprungliga syftet. Detta ger än mer makt åt de övervakande; skrupellösa tjänstemän kan använda information till utpressning, oavsett om det är av politiska skäl eller av ekonomisk egennytta. Det öppnar också upp för möjligheten till selektiva godtyckliga åtal eller utlämnande av laglig, men pinsam, aktivitet för att påverka den misstänkte.[145]

I Storbritannien används övervakningskameror (en kamera per 14 invånare) [146] för att styra befolkningen mot handel, och bort från allt från brott till protester. Det finns ett system med ”anti-social behaviour orders”, som används för att förflytta grupper med tonåringar som inte handlar bort från kommersiella stadskärnor, för att säkerställa att handeln sker effektivt.[147]

Neils lösningsförslag på den problematik han ser är följande:

1. Gör det svårare för företag att bygga databaser, och försvåra utbytet mellan statliga och privata databaser.[148]
2. Hemliga övervakningssystem, vars själva existens hålls hemlig, är illegitima. Hemlig övervakning i sig ska dock fortsatt tillåtas.[149]
3. Total övervakning av all kommunikation är illegitim, då det finns potential för massivt missbruk. Det måste finnas en meningsfull rättslig prövning innan övervakning av internet auktoriseras.[150]
4. Vi måste se övervakning som något skadligt, det ska krävas en hög tröskel för att staten skall få tillgång till arkiv på internet innehållande exempelvis sökhistorik och e-post.[151]

Han anser att det inte längre är science fiction med en värld av total övervakning; den rycker tvärtom allt närmre allt eftersom programvara

[142] Richards, Neil, The Dangers of Surveillance s. 28-29
[143] Ibid s. 29-30
[144] Ibid s. 30
[145] Ibid., s. 31
[146] Lessons from the British and American Approaches to compelled decryption, s. 362
[147] Richards, Neil, The Dangers of Surveillance s. 31-32
[148] Ibid. s. 35-38
[149] Ibid. s. 38-39
[150] Ibid. s. 40
[151] Ibid. s. 41

kodas, databaser kombineras och varje ny övervakningskamera läggs till nätverket.[152] Han citerar ett uttalande om att det idag är möjligt att köra en approximation av ”1984” på ett par servrar.[153]

4.2.3 Rekommendation 3/97 - Anonymitet på internet

Neils resonemang om ”Big data” är av stor betydelse för min uppsats, och jag ska därför kort belysa detta närmre genom ytterligare ett exempel från verkligheten. I Europakommissionens rekommendation 3/97 – Anonymitet på internet diskuterar man redan 1997 möjligheterna som analyserandet av transaktionsdata ger upphov till. Transaktionsdata förklaras som den data som uppstår när en användare gör musklick på de artiklar han vill läsa, till skillnad mot TV och tidningar. En person som använder internet lämnar på så vis spår efter sig, som gör att ”handlingar, val och preferenser kan registreras.”[154]

Bara genom att utnyttja program som automatiskt söker upp och databehandlar all allmänt tillgänglig information om en namngiven, slumpvis utvald person i olika diskussionsgrupper, är det möjligt att få tag på mycket information, framhålls i dokumentet: ”Tidningen kunde få tag på personens adress och telefonnummer, födelseort, studieort, yrke, nuvarande arbetsplats, hans intresse för amatörteater, favoritöl, favoritrestauranger och -resmål samt hans åsikter om så varierande ämnen som Bill Gates och det sociala förtrycket i delstaten Indiana.” [155].[156]

Det blir här uppenbart vilken betydligt mer komplett profil av en person man snabbt skulle kunna göra om även information som personen aktivt försöker hålla hemlig, exempelvis anonyma bloggar och foruminlägg, tillsammans med information staten kan komma åt, som allt internetanvändande samt information i e-post och telefonsamtal, läggs till profilen, kombinerat med ansiktsigenkänning från övervakningskameror, positionsbestämningar via mobiltelefon, osv.

I det här sammanhanget bör man också ha klart för sig hur fort, men framförallt hur stadigt, teknikutvecklingen går. I slutet av 1993, det år rekommendationen skrevs, kunde den snabbaste superdatorn i världen hantera 1 338 000 000 000 beräkningar per sekund, i år ligger den summan istället på 33 862 700 000 000 000.[157] I dagsläget finns det inget direkt hinder mot att utvecklingen skulle fortsätta, tvärtom har den hittills gått exponentiellt[157] och accelererar därmed hela tiden, varför det redan

[152] Richards, Neil, The Dangers of Surveillance s. 40
[153] Ibid. s. 30
[154] Rekommendation 3/97, Anonymitet på Internet, s. 4
[155] Ibid s. 5
[156] Ibid. s. 4-5
[157] http://www.top500.org/statistics/perfdevel/

diskuteras planer på datorer med tiotals gånger högre prestanda som kan stå färdiga om ett antal år.[158]

Oöverstigliga hinder som kanske finns idag när det gäller möjligheten att koppla ihop information från olika källor, automatiskt känna igen ansikten från övervakningskameror, och se stora samband och mönster i ostrukturerad information och skapa exempelvis sociogram, kan därför vara bagatellartade att lösa endast ett par år framåt i tiden, något jag anser att det är viktigt att komma ihåg vid utformandet av hållbara juridiska lösningar för framtiden.

4.2.4 Motståndare till anonymitet

Ett mer uttalat motstånd till anonymitet kommer ibland från oväntat håll. 2011 gick exempelvis chefredaktören för tidningen Norran ut i en debattartikel där hon ifrågasatte möjligheten till att vara anonym på nätet till hinder för lagföring.[159] Till samma resultat kommer filosofen Tännsjö, om än på helt andra grunder. Han anlägger ett närmast deterministiskt perspektiv på övervakningen, den är omöjlig att stoppa, istället bör man skapa ett system av total öppenhet i båda riktningarna mellan enskilda och staten.[160]

När jag började arbetet med min uppsats skickade jag ut ett brev[161] till flera filosofiska fakulteter, där jag tog upp den problematik jag såg med övervakning och undrade vilka filosofiska ståndpunkter kring anonymitet och integritet som debatterades i den filosofiska litteraturen. Till min stora förvåning fick jag bara ett svar, som hänvisade till just Tännsjös artikel.

Motstånd mot möjligheten till kryptering av information kommer också från mer förutsägbart håll, åklagare har tidigare gått ut och påtalat svårigheterna med att information krypterats så den är omöjlig att ta del av, så att den förblivit skyddad trots att tillstånd funnits att övervaka den. Man har därför önskat metoder för att få den dekrypterad. I samma artikel pekar Anders Ahlqvist, IT-brottsspecialist på Rikspolisstyrelsen, att det i praktiken är omöjligt att dekryptera information, utan det som behövs är hemlig dataavläsning för att få tag på informationen innan den dekrypteras.[162] Man har från åklagarhåll även tidigare önskat metoder mot kryptering.[163]

[158] http://edition.cnn.com/2012/03/29/tech/super-computer-exa-flop/
[159] http://www.svd.se/kultur/kulturdebatt/anonymiteten-skapar-trollen_6375562.svd
[160] http://www.dn.se/debatt/lat-oss-bejaka-maktens-overvakning-av-vara-liv/
[161] Bilaga 1
[162] http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5241785
[163] http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5618974

4.2.5 Replik på Tännsjös artikel

I en direkt respons[164] till Tännsjös debattartikel går tre forskare till gemensamt angrepp mot den syn på övervakningssamhället som han presenterar. De framhåller att informationstekniken erbjuder flera lösningar för att undgå ett övervakningssamhälle, bortsett från de av mig tidigare nämnda krypteringstjänsterna för att skydda kommunikation nämner de även anonym publicering via Wikileaks.

De poängterar att det därmed är en politisk fråga om samhället vill använda den framväxande tekniken för att säkra människors privata sfär, eller om vi ska fortsätta att utnyttja den för att bygga upp ett övervakningssamhälle.

De för slutligen fram kritik mot det synsätt på ömsesidig transparens som Tännsjö argumenterar för. Den idén är inte applicerbar på dagens övervakning, till skillnad mot förr när det fanns en mapp med analyserad data om den enskilde individen som denne i teorin kunde få en möjlighet att läsa, sparas nu ”allt som går att samla in”. Det rör sig om flera gigabyte rådata, som mobilpositioner, som bara blir relevant först om den samkörs med data från andra individer samt exempelvis data om mobilmasters placeringar.[165] De menar dessutom på att resonemanget om att transparens i båda riktningarna mellan staten och den enskilde som en lösning är felaktigt, istället menar de att ”transparensen ökar skevheten”.

4.2.6 Övriga synpunkter

Jag har även valt att titta på andra synpunkter på övervakning. Anne-Marie Eklund-Löwinder, chefen på stiftelsen .SE, anser att en rätt till anonymitet på internet är nödvändigt för att garantera yttrandefrihet.[166] Till samma slutsats kom en del av den svenska scoutrörelsen, med följden att de upprättade en anonymitetstjänst liknande TOR.[167] Även piratpartiet har varit med och startat upp en anonymitetstjänst.[168] Det är min uppfattning efter att ha följt debatten kring införandet av exempelvis datalagringsdirektivet och den s.k. ”Ipred-lagen” att det dessutom allmänt finns en relativt stor polarisering i samhället om anonymitet på internet skall vara fortsatt möjlig eller inte.

Det kan avslutningsvis vara relevant att kort nämna den kraftigt svängande syn på integritet som skett, i ett yttrande om Europarådets konvention om cyberbrottslighet tar arbetsgruppen för uppgiftsskydd upp att det vid ett möte för EU:s dataskyddsansvariga år 2000 sågs som orimligt att internetleverantörer rutinmässigt skulle behålla trafikuppgifter och ge rättsväsendet tillgång till dessa, det ansågs av dessa dessutom stridande mot

[164] http://www.sydsvenskan.se/opinion/aktuella-fragor/det-vore-fullt-mojligt-for-politiken-att-framja-sadana-tekniker-istallet-for-a/
[165] Alltså ett användande av någon form av ”big data”, min anmärkning.
[166] https://www.iis.se/blogg/anonym-pa-natet/
[167] http://cybernormer.se/scouter-kopplar-internet-till-manskliga-rattigheter/
[168] http://pcforalla.idg.se/2.1054/1.72937

Europakonventionen. Arbetsgruppen menade också på att det höll på att uppstå ett sådant konsensus kring frågan.[169] Ett antal år senare genomdrevs istället datalagringsdirektivet.

4.2.7 Missbruk och faror med övervakningssystem

Under tiden McCarthy var president samarbetade FBI med kongressen i en jakt på vissa grupper av personer, de med kommunistanknytning, ”allmänt oamerikanska åsikter” eller som bara hade ”en opassande livsstil”. Man utnyttjade sig av ett informellt och i stort sett osynligt system för personkontroll som tillsammans med FBI:s register användes för att dels neka amerikanska medborgare pass, dels varna arbetsgivare. Resultatet blev i praktiken detsamma som ett yrkesförbud. [170]

Under 1950-talet när FBI stod på toppen av sin makt startades ett nytt program, Cointelpro, för att bekämpa motståndares organisationer och deras nyckelpersoner. Man skulle slå till innan brotten hunnit begås, planeras eller ens övervägas. Högst prioritet hade det amerikanska kommunistpartiet, detta bestod av falanger som stred sinsemellan, och FBI som genom avlyssning och infiltratörer visste vilka intriger som var aktuella kunde elda på konflikterna med provokationer, anonyma brev och direkta personangrepp. Man avsatte exempelvis effektivt en ledande partifunktionär genom att lägga en kopia av en angivarraport i hans bil, så att andra medlemmar i partiet kunde upptäcka den. Detta resulterade i att partifunktionären helt uteslöts ur partiet.[171]

Under 1960-talet började man istället använda programmet mot vad man ansåg var nya hot mot samhället, bland annat medborgarrättsrörelsen inkluderande Marthin Luther King och den ökande kritiken mot Vietnamkriget. Man tog allt mer på sig rollen som ”hemlig politisk aktör med subversiva och i många fall direkt olagliga metoder”[172]. Hoover, som då styrt FBI i närmre 50 år, styrde utan insyn utifrån, och ingen president vågade sätta sig upp emot honom. President Richard M Nixon försökte 1971 två gånger att avskeda honom, men båda gångerna misslyckades han. Orsaken var att Hoover skaffat sig en oerhörd makt genom information, han hade tillgång till förödmjukande information om alla som kunde tänkas bli en motståndare, presidenterna inräknade.[173]

4.3 Europadomstolens syn på integritet

Europadomstolens syn på integritet är som sagt viktig. Jag kommer därför att först gå igenom Europadomstolens tolkningsmetoder, därefter praxis i form av ett antal utvalda rättsfall. Jag har valt ut dessa eftersom jag anser att

[169] Yttrande 4/2001 om Europarådets utkast till konvention som cyberbrottslighet, s. 7
[170] Agrell, Willhelm, FBI – brottslighetens främsta fiende, 2008, stycke 8
[171] Ibid stycke 9
[172] Ibid stycke 10
[173] Ibid stycke 9, 13

de sammantaget klart visar hur domstolen verkar se på frågan om personlig integritet i förhållande till ingripande hemliga tvångsmedel, och hur en förändring i den synen skett under åren.

4.3.1 Europadomstolens tolkningsmetoder

Artikel 8 - Rätt till skydd för privat- och familjeliv
1. Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens.
2. Offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.[174]

Det ligger i ett hemligt tvångsmedels natur att det inkräktar på den personliga integriteten, såsom den tar sig uttryck i Europakonventionens artikel 8. Artikeln är givetvis inte utan undantag, utan redan i artikelns andra punkt tas de undantag upp som motiverar en inskränkning i principen.

För att ett ingrepp i den sfär som artikel 8 skyddar ska accepteras, krävs det att ingreppet går in under undantagsbestämmelsen i artikel 8:2.[175]

För att detta ska vara uppfyllt, måste tre förutsättningar vara uppfyllda, nämligen:

1. Ingreppet måste ha stöd i lag
2. Ingreppet måste ha till syfte att säkra något av de intressen som räknas upp i art 8.2
3. Ingreppet måste slutligen vara nödvändigt i ett demokratiskt samhälle. Domstolen har angående punkten 3 sagt att nödvändigt inte är synonymt med oundgängligt, det krävs dock som sagt ett "pressing social need".[176]

Det är den sista bedömningen, utvärderingen av demokratisk nödvändighet, som har fött den mest betydelsefulla principen, nämligen proportionalitetsprincipen.[177] Den går ut på att det måste finnas ett rimligt förhållande mellan ett mål som man vill uppnå, och de medel man använder för att uppfylla målet.[178]

Den sista punkten är uppenbarligen mer öppen för tolkning än de övriga, och därför som tidigare nämnts intressantast för min uppsats. Domstolen har

[174] Europeiska konventionen om skydd för de mänskliga rättigheterna, artikel 8
[175] Danelius, Hans, Mänskliga rättigheter i Europeisk praxis, 2000 s. 223
[176] http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp interpretative principles, kapitel 1 p.3
[177] Ibid kapitel 1 p. 3c
[178] Ibid kapitel 1 punkten 4

uttalat att följande frågor måste ställas i fall som rör nödvändigheten av intima aspekter av privatlivet:[179, 180]

3.1. Existerar det ett tvingande socialt behov av en inskränkning av en konventionsrättighet?
3.2. Om så är fallet: korresponderar den ifrågavarande restriktionen till behovet?
3.3. Om så är fallet: Är det en proportionerlig respons till behovet?
3.4. Oavsett, är skälen framlagda av myndigheterna relevanta och tillräckliga?

Det är som synes ett viktigt krav att en åtgärd korresponderar till behovet. I svensk rätt har man beskrivit proportionalitetsprincipen som den kommer till utryck i EG-rätten och Europakonventionen som att den innefattar ett krav på ändamålsenlighet och lämplighet, det aktuella ingreppet skall vara ägnat att tillgodose det avsedda ändamålet.[181] I ett yttrande framhåller även Internationella juristkommissionen vikten av att en åtgärd är ändamålsenlig.[182]

Det är dock upp till de nationella organen att göra den första bedömningen om det finns ett tvingande socialt behov, något som ger dessa en viss "margin of appreciation", en viss frihet att själva avgöra behovet. Den frihet staterna ges är dock inte oinskränkt, det är slutligen upp till Europadomstolen att bedöma om friheten utnyttjas på ett bra sätt.[183]

Hur stor frihet staten har varierar från fall till fall. När det gäller skyddet för den nationella säkerheten har staten en större frihet än vad den har vid exempelvis homosexuellas rättigheter, som inte är ett område av fundamental betydelse för en konventionsstat.[184]

Till detta kommer också att:

1. Syftet med Europakonventionen är att skydda enskilda individer, man ska alltså inte se till staternas intresse av att konventionen hålls såsom det avtal den är. Den skall alltså inte tolkas restriktivt för att skydda enskilda staters suveränitet.[185]

2. Ansvaret ligger på staten, Europadomstolen är inte en fjärde instans.[186]

---

[179] Foster, Steve, Human rights and civil liberties, Storbrittanien, 2008. s. 58
[180] http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp kapitel 1 p.4
[181] RÅ 1999 ref. 76 punkten 5.5.1
[182] Internationella Juristkommissionen, yttrande över DS 2011:44, s. 2
[183]http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp kapitel 1
[184] Danelius, Hans, Mänskliga rättigheter i Europeisk praxis, 2000, s. 224
[185] http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp kapitel 1 p1
[186] Ibid kapitel 1p2

3. Det måste dessutom kunna visas att den lagstiftning ett land inför som inskränker ett intresse som skyddas i konventionen, verkligen i det specifika fallet använts i det syftet mot den som klagar hos Europadomstolen. Det är alltså inte tillåtet att använda lagstiftning som förvisso kommit till med ett legitimt syfte för något annat än det var tänkt.[187]

4.3.2 Praxis rörande artikel 8 – Telefonavlyssning

Den uppfattning jag fått under tiden som jag har arbetat med den här uppsatsen är att det finns förhållandevis lite praxis kring artikel 8 och olika former av hemlig avlyssning, när det kommer till att avgöra om inskränkningen är nödvändig i ett demokratiskt samhälle. Den rättspraxis som finns berör främst om en metod har klart stöd i lag, inte om den är proportionerlig, detta eftersom Europadomstolen oftast låter bli att svara på om en inskränkning är proportionerlig om de dessförinnan kommit fram till att den ej har tydligt stöd i inhemsk lag.[188]

När man läser litteratur inom ämnet finns det heller i princip inga hänvisningar till att proportionalitet är ett problem när det kommer till frågan om olika hemliga tvångsmedel över huvud taget skall godkännas, utan det intryck jag får är att Europadomstolen, trots de ovan redovisade tolkningsmetoderna, präglas av en utpräglad låt-gå attityd i det fallet.[189]

Jag har trots detta hittat ett antal enligt mig intressanta rättsfall för att belysa frågan om hur domstolen ser på motsättningen mellan nödvändighet i ett demokratiskt samhälle och om det är en proportionerlig respons. Dessa är det äldre fallet **Klass m.fl. mot Tyskland**, samt det nyare **Kennedy mot England.** Jag har dessutom valt att ta med fallet **Malone mot England**, då domstolen trots allt gör vissa intressanta uttalanden där, som är upplysande för hur domstolen egentligen resonerar.

4.3.2.1 Klass m.fl. mot Tyskland

Ett antal tyska medborgare, främst advokater och domare, hade valt att föra talan mot ny tysk lagstiftning som gjorde det möjligt att bl.a. avlyssna telefonsamtal och öppna brev.[190]

De hävdar inte att staten inte har rätt att använda sig av sådan lagstiftning, utan vänder sig mot det faktum att det varken finns möjlighet att föra talan vid domstol mot vare sig beslutet att använda tvångsmedlen eller själva användandet av tvångsmedlen, samt att myndigheterna inte i efterhand

[187] http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp kapitel 1 p 3b
[188] Murphy, Maria, The relationship between the European Court of Human Rights and National Legislative Bodies, Irish Journal of legal studies, Vol 8(2) s. 75
[189] Jmf. exempelvis Ehrenkrona, Carl-Henrik, Lagkommentar Lag 1994:1219, not 51, Karnov
[190] Klass m.fl mot Tyskland (application no. 5029/71) p.10

måste berätta att de använt sig av tvångsmedlen.[191]

Den tyska författningsdomstolen förklarade lagen ogiltig i den del den inte tvingade staten att avslöja att tvångsmedlet använts ens när det kunde ges en notifikation utan fara för ändamålet med avlyssningen.[192]

Den tyska lagstiftningen innebar att man i vissa fall inte behövde meddela den misstänkte, nämligen "to protect the free democratic constitutional order or the existence or security of the Federation or of a Land".[193]

Utifrån detta infördes möjligheten att avlyssna telefonsamtal, öppna brev, läsa telegrafmeddelanden etc. i vissa angivna situationer, då det behövs för att skydda exv. "den demokratiska konstitutionen", "existensen eller säkerheten av federationen eller en delstat", eller "de allierade truppernas säkerhet" från ett omedelbart hot. Dessutom behövde två ytterligare förutsättningar vara uppfyllda: dels faktiska indikationer för att misstänka en person för att planera, utföra eller ha utfört vissa straffbelagda handlingar, såsom brott mot statens säkerhet eller den demokratiska ordningen, dels måste andra metoder för att utreda brottet vara betydligt svårare eller vara helt utan möjlighet till framgång. Övervakningen får bara beröra den misstänkte eller sådana andra personer som, baserat på klar fakta, misstänks ta emot eller vidarebefordra kommunikation åt den misstänkte, eller den vars telefon den misstänkte presumeras använda.[194]

En stor del av domstolens avgörande tar upp och beskriver den beslutskedja och de organ som tar tillvara den misstänktes intressen. För att försäkra sig om att inte ändamålet med åtgärderna går om intet meddelas inte personen efter att avlyssningen slutat, och det finns inget effektivt rättsmedel för att få reda på om avlyssning har skett eller för att bestrida användandet.[195]

Domstolen kommer fram till att det för alla de personer som lagstiftningen teoretiskt skulle kunna appliceras på det finns ett ”menace of surveilance” som slår mot friheten att kommunicera genom post och telefon, och därigenom är den ett ingrepp i artikel åttas skyddssfär.[196]

Domstolen kommer fram till att själva huvudfrågan under artikel 8 är om inskränkningen av artikeln kan rättfärdigas i enlighet med art 8.2. Eftersom det rör sig om en inskränkning av en rättighet enligt konventionen ska paragrafen tolkas restriktivt. Domstolen konstaterar att: "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.".[197]

---

[191] Klass m.fl mot Tyskland (application no. 5029/71) p.10
[192] Ibid p. 11
[193] Ibid p. 16
[194] Ibid p. 17
[195] Ibid p. 18-24
[196] Ibid p. 41
[197] Ibid p. 42

För att inte vara ett brott mot artikel 8 måste åtgärderna ha stöd i lag, vilket domstolen finner vara fallet.[198] Domstolen finner också att lagstiftningens mål är något av de accepterade undantagen i artikel 8.2.[199] Domstolen går därefter vidare till att se om lagstiftningen dessutom håller sig inom vad som är nödvändigt i ett demokratiskt samhälle.[200]

Domstolen konstaterar i den delen till att börja med, i bedömningen av artikel åttas skyddssfär, att man inte kan undvika att notera två viktiga saker. Dels de teknologiska framsteg som har skett inom spionerі och därmed även inom övervakning, dels framväxandet av terrorism i Europa:

> "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[201]

Domstolen konstaterar dock också att detta inte innebär att staten har en obegränsad frihet att utsätta medborgare inom dess gränser för hemlig övervakning, domstolen är medveten om "the danger such a law poses of undermining or even destroying democracy on the ground of defending it" och konstaterar att staterna inte i striden mot spionerі och terrorism får använda vilka medel de vill.[202]

Man säger vidare att det måste finnas adekvata och effektiva garantier mot missbruk. Om så bedöms vara fallet beror på flera faktorer, bland annat naturen av, omfånget och varaktigheten av de möjliga medlen, vilka myndigheter som kan bevilja, utföra och övervaka dem, samt vilka rättsmedel som finns att tillgå hos de nationella myndigheterna.[203]

Domstolen konstaterar här att systemet som sagt bara får användas vid vissa allvarliga brott, att det bara får användas när andra möjligheter inte står till buds, etc. "Explorative surveillance" tillåts inte.[204] Trots att det bästa vore om systemet övervakades av en domare är den tyska modellen tillräcklig då de som övervakar den har tillräcklig kompetens och makt.[205]

Domstolen finner därför inget brott mot artikel 8.[206]

---

[198] Klass m.fl mot Tyskland (application no. 5029/71) p.43
[199] Ibid p. 44-46
[200] Ibid p. 46
[201] Ibid p. 48
[202] Ibid p. 49
[203] Ibid p. 50
[204] Ibid p. 51
[205] Ibid p. 56
[206] Ibid p. 60

4.3.2.2 Malone mot England

Malone arbetade som antikhandlare, han blev åtalad för att ”oärligt ha hanterat stulet gods”. Juryn kunde dock inte enas, utan han blev frikänd.[207]

Under rättegången visade det sig att detaljer från ett telefonsamtal som Malone hade haft fanns i ett anteckningsblock tillhörande den polis som ledde utredningen. Åklagarsidan bekräftade att den konversationen avlyssnats med stöd av ett föreläggande från "secretary of state for the home department".[208]

Malone sökte på grund av detta i en rättprocess försöka få fastslaget att övervakningen av hans telefon varit olaglig, oavsett om det fanns ett föreläggande eller inte. Detta avslogs dock.[209] Han gjorde också gällande att han trodde att hans telefon och korrespondens avlyssnats under en längre period. Regeringen ville dock inte kommentera detta i syfte att skydda informatörer. Man bekräftade dock att då Malone var misstänkt för att ha tagit emot stulet gods, tillhörde han därmed den krets av personer som kunde utsättas för avlyssning.[210]

Han trodde också att hans telefon hade utrustats med en apparat för att spara alla nummer som ringts från denna (”metering”), detta då tjugo personer som han tidigare hade ringt hade utsatts för husrannsakan efter att han gripits. Regeringen nekade till att detta skulle vara fallet.[211]

En mycket stor del av domen går åt till att förklara det engelska systemet för att godkänna telefonavlyssning. Domstolen kommer slutligen fram till att den engelska lagstiftningen i den här delen inte är tillräckligt tydlig.[212] Därför är inte inskränkningen av artikel 8 i enlighet med kravet på ”enligt lag” i 8.2.[213]

Domstolen går därefter in på frågan om avlyssningen av kommunikation är nödvändig i ett demokratiskt samhälle. Man uttalar att det utan tvivel är så att någon form av möjlighet för polisen att avlyssna kommunikation kan vara en nödvändighet i ett demokratiskt samhälle för att hindra oordning och brott. Domstolen säger sig till exempel acceptera regeringens påstående om att ökningen av brott, och särskilt ökningen av organiserad brottslighet, de allt mer sofistikerade kriminella och lättheten och snabbheten de kan förflytta sig på har gjort telefonavlyssning till ett oumbärligt hjälpmedel i utredandet och preventionen av allvarliga brott. På grund av dess ofrånkomliga sekretess, kan sådana hjälpmedel dock missbrukas på ett sätt som potentiellt är lätt i det enskilda fallet och kan ha skadliga konsekvenser

[207] Malone mot England (application no. 8691/79) p. 12-13
[208] Ibid p. 14
[209] Ibid p. 15
[210] Ibid p. 16
[211] Ibid p. 20
[212] Ibid p. 79 stycke 3
[213] Ibid p. 80

för det demokratiska samhället som helhet. Man konstaterar på de grunderna att det bara kan klassas som nödvändigt i ett demokratiskt samhälle om systemet för hemlig övervakning innehåller tillräckliga garantier mot missbruk, man hänvisar här till fallet Klass.[214]

Då domstolen konstaterat att det engelska systemet för avlyssning inte var "i enlighet med lag", anser man sig dock inte behöva pröva detta vidare.[215]

När det gäller processen med "metering" så kommer man fram till att det saknas tydligt lagstöd om i hur stor omfattning myndigheterna har rätt att använda sig av metoden, och på vilket sätt. Därför är inte heller systemet med "metering" i enlighet med konventionen.[216]

Till skillnad från den tidigare frågan går domstolen här över huvud taget inte in på om "metering" är nödvändigt i ett demokratiskt samhälle, då man redan kommit fram till att systemet saknade tydligt lagstöd.[217]

Concurring opinion, Judge Pettitti

Domare Pettitti håller med övriga om intrånget i artikel 8, men har en del att tillägga. Han hade velat att man trots allt undersökt hur det engelska systemet stod sig under 8.2 vad gäller adekvata garantier mot missbruk och inte uteslöt den bedömningen såsom onödig efter att ha kommit fram till att det engelska systemet inte uppfyllde Europakonventionens krav på ”i enlighet med lag”.[218]

Han anser detta på grund av en summering av flera omständigheter han anser vara för handen mellan 1980-1990, vid tiden för domen.[218]

Demokratiska stater hotas allt oftare av att offentliga myndigheter vill "se in i" medborgarnas liv. För att kunna planera och få skatte- och socialpolitik att fungera behöver staten förstärka sina ingrepp. Man behöver föröka och datorisera information om personer.[218]

I ett nästa steg försöker staten bygga upp en profil av varje medborgare. Undersökningar blir vanligare, och telefonavlyssning utgör ett av de favoriserade medlen för den "permanenta undersökningen".[218]

Han menar att användandet av datorer gör telefonavlyssning oerhört mycket effektivare, resultatet kan lagras på magnetiska band och processas i exempelvis postcenter. Man kan därmed utöka antalet telefonavlyssningar hundrafaldigt och analysera dem inom allt kortare tidsrymder. Han anser också att det vore förhastat att tro att det i varje land bara sker ett par hundra

[214] Malone mot England (application no. 8691/79) p. 81
[215] Ibid p. 82
[216] Ibid p. 87
[217] Ibid p. 88
[218] Ibid s. 38

telefonavlyssningar per år och att myndigheterna vet om alla.[219]

Vid sidan av teknikutvecklingen anser han att myndigheternas mål diversifierats; bortsett från avlyssning för att förhindra brott sker avlyssning av politiska skäl, journalister och ledande personer avlyssnas. Detta bortsett från avlyssning av underrättelsetjänster som klassas som ”top secret”, och som han menar varken domen eller hans tillägg berör.[220]

Han menar att de flesta medlemsstater har känt ett behov av att introducera lagstiftning på området för att få slut på det växande missbruk som även hotade dem med makt. Han konstaterar att den lagstiftningsmetod som oftast använts är en brottsmålsprocedur, där en domare fattar beslut och kontrollerar användandet, liksom vid en husrannsakan.[220]

Det brittiska systemet lade istället den makten hos minister of the interior.[220]

Domare Petitti hade velat att man kom fram till att det brittiska systemet stred mot 8.2 eftersom det ej fanns någon domstolkontroll över hur systemet utnyttjades, han menar att oavsett om det finns tydlig lagstiftning finns det en risk att systemet kan bli rättsosäkert utan den kontrollen.[221]

Han anser att domstolen kunde ha gjort en distinktion mellan fallet Klass å ena sidan, som rörde krissituationer till följd av terrordåd, och det nuvarande fallet, som rörde vanliga brott. Han konstaterar att intrång till följd av avlyssning av kommunikation är värre än andra intrång i rättigheter, eftersom det oskyldiga offret inte har någon chans att upptäcka det.[221]

Han anser att det är lika illa att utsättas för avlyssning mot ens vilja som att inte kunna stoppa avlyssningen när den är illegal eller oberättigad.[222]

Han hänvisar till vad man sa om avlyssning i Klass-målet, att eftersom artikel 8.2 ger möjligheter till inskränkningar av en garanterad rättighet, den ska tolkas snävt och att "powers of secret surveillance of citizens, characterising as they do the police State, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions"[223]. Han menar att om man då lämnar kontrollen över bedömningen av graden av farlighet eller misstanke till polisen, även under kontroll av Home office, kan det inte klassas som ett adekvat medel konsistent med målet man försöker uppnå, även om målet i sig är legitimt, och oavsett är systematisk avlyssning av kommunikation i avsaknad av en opartisk, självständig och rättslig kontroll disproportionerlig i förhållande till målet man försöker uppnå.[224]

[219] Malone mot England (application no. 8691/79) s. 38-39
[220] Ibid s. 39
[221] Ibid s. 40
[222] Ibid s. 41
[223] Ibid s. 43
[224] Ibid s. 42-43

Han menar på att även om staterna utan tvekan måste ha rätt att själva ha en inhemsk handlingsfrihet, och att den kan variera i omfång beroende på vilket mål i artikel 8 och 10 som berörs, så faller rätten till privatliv i förhållande till verkställande myndigheter in i den mest krävande kategorin av konventionsrättigheter och medför därför en viss restriktion när det gäller den inhemska handlingsfriheten.[225]

Han konstaterar att fast domstolen med rätta konstaterat att "metering" är ett ingrepp i det område som skyddas av artikel 8.1, så skulle man även här ha kunnat ge en dom genom att applicera artikel 8.2, med informationen kan staten få reda på saker som det inte var menat att den skulle veta.[225]

Han avslutar sitt tillägg med att Malone-domen är ett led i en kontinuerlig kedja av domar där domstolen agerar väktare av konventionen. Domstolen uppfyller den rollen genom att undersöka artikel 8 i sin fulla dimension och genom att begränsa "the margin of appreciation" särskilt i de områden där individen är mer och mer utsatt som ett resultat av modern teknik. Erkännandet av hans rätt att bli "lämnad ifred" är inneboende i artikel 8. Konventionen skyddar gemenskapen av människor, människan i vår tid har ett behov av att bevara sin identitet, att vägra den totala öppenheten av samhället, att bibehålla integriteten av sin personlighet.[226]

4.3.2.3 Kennedy mot England

Fallet rör ett klagomål från Kennedy, efter en uppmärksammad mordrättegång, där han hävdade att han blivit oskyldigt dömd efter att poliser vittnat falskt för att dölja deras egna brott, misstänkte han att hans telefon avlyssnades. Han grundade detta på tidsödande bluffsamtal och samtal som inte kopplades fram till honom, och trodde att orsaken var de tidigare händelserna samt att han drev en kampanj mot justitiemord. Han misstänkte att myndigheterna kontinuerligt och olagligt förnyade en avlyssningsorder, detta för att skrämma honom och underminera hans affärsverksamhet.[227]

Han försökte ta reda på om det fanns information om honom som processades hos Secret service i England, men nekades att ta del av informationen, detta med hänvisning till nationell säkerhet.[228]

Han lämnade senare in två klagomål till ”the Investigative Powers Tribunal” (IPT), över att hans kommunikation avlyssnades. Dels för att den enligt honom avlyssnades under förhållanden den inte skulle ha gjorts, dels för att avlyssningen stred mot Europakonventionens artikel 8.[229]

---

[225] Malone mot England (application no. 8691/79) s. 43
[226] Ibid s. 43-44
[227] Kennedy v. England (application no. 26839/05) p. 5-7, 99
[228] Ibid p. 8
[229] Ibid p. 9, 100

Tribunalen kom fram till att ”no determination had been made in his favour in respect of his complaints”[230], vilket kunde betyda att det antingen inte hade varit fråga om någon avlyssning, eller att den avlyssning som skett var laglig.[230] Formuleringen användes för att kunna upprätthålla en ”varken bekräfta eller dementera-policy” rörande hemlig avlyssning.[231]

Den engelska lagstiftning som är aktuell i fallet bygger på att avlyssning endast får ske om det behövs för att skydda Englands ekonomiska intressen, hindra eller upptäcka allvarlig brottslighet eller behövs för den nationella säkerheten. Det krävs dessutom att åtgärden är proportionerlig till det man försöker uppnå.[232] Det finns också en skyldighet att överväga om informationen man vill åt kan kommas åt på något annat vis.[233]

“National security” definieras som: “[activities] which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means.”[234]

“Serious crime” definieras som ett brott där den som utför det, som är 21 år och aldrig tidigare dömd, rimligtvis kan dömas till tre års fängelse. Också brott som utförs av en stor grupp för ett gemensamt mål, som kan innebära stor finansiell vinning, eller involverar våld räknas in i den kategorin.[235]

Det finns en kommissionär som ska övervaka hur systemet sköts, denne är en person som innehar eller har innehaft ett högt domarämbete. Hans uppgift är att tillse att systemet sköts ordentligt, de som auktoriserar eller verkställer avlyssningsbeslut är skyldiga att lämna ut all information till honom som han begär. [236]

IPT inrättades för att undersöka klagomål från medborgare om felaktig avlyssning av deras kommunikation som ett resultat av lagstiftningen. Medlemmarna måste inneha eller ha innehaft ett högt domarämbete eller varit kvalificerad advokat i minst 10 år. Alla kan lämna in ett klagomål till IPT, och de måste avgöra alla.[237]

Man motiverar policyn med att varken dementera eller bekräfta bland annat med att övervakningen som sådan, men även metoderna, måste hållas hemliga. I fall där information om hemliga avlyssningsmetoder kommit ut till allmänheten, har detta lett till förluster av viktiga källor till information.[238]

[230] Kennedy v. England (application no. 26839/05) p. 20
[231] Ibid p. 137
[232] Ibid p. 31-32
[233] Ibid p. 36
[234] Ibid p. 33
[235] Ibid p. 34
[236] Ibid p. 57-58
[237] Ibid p. 5
[238] Ibid p. 137

Domstolen konstaterar att en inskränkning i artikel 8 bara kan motiveras enligt artikel 8:2 om den är i enlighet med lag, verkar för ett eller flera av de legitima målen enligt artikeln, och är nödvändig i ett demokratiskt samhälle för att uppnå ett sådant mål.[239]

Domstolen tar återigen upp fallet Klass, och uttalandet där om att powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. Man säger dock att innebörden av detta i praktiken är att det måste finnas effektiva och adekvata garantier mot missbruk. Om så är fallet beror på alla omständigheter i fallet, som naturen, längden och omfattningen av åtgärderna, skälen för att begära dem, vilka myndigheter som kan beordra dem, verkställa och övervaka dem, och vilka rättsmedel som finns tillgängliga hos de nationella domstolarna.[240]

Domstolen konstaterar att man har erkänt staternas rätt till en viss "margin of appreciation" när det kommer till att bedöma existensen och vidden av den nödvändigheten, men att bedömningsmarginalen ligger under europeisk tillsyn. Domstolen har att bedöma om proceduren för beordran och övervakning av åtgärderna är tillräckliga för att hålla åtgärderna till vad som är nödvändigt i ett demokratiskt samhälle.[241]

På grund av att domstolen tagit upp klagandens generella klagomål på lagstiftningen som ligger till grund för avlyssningen, och inte någon avlyssning som påstås ha skett, får domstolen i sin bedömning av om åtgärderna är tillåtna enligt artikel 8.2, se på proportionaliteten av lagstiftningen i sig och säkerhetsåtgärderna inbyggda i systemet som tillåtit hemlig övervakning, istället för att titta på proportionaliteten av några specifika åtgärder riktade mot den klagande. Domstolen kommer fram till att det i sammanhanget är så att lagligheten av åtgärderna är nära länkat till frågan om nödvändighetstestet uppfyllts i fråga om den engelska lagstiftningen. Man väljer därför att utreda kraven på "nödvändigt i ett demokratiskt samhälle" tillsammans med "i enlighet med lag".[242]

Man kommer fram till att lagstiftningen syftar till ett legitimt mål, nämligen till att skydda nationell säkerhet, bekämpa brottslighet samt skydda landets ekonomiska välstånd. Man kommer efter en lång analys även fram till att lagstiftningen är tillräckligt klar, och inskränkningen av artikel 8 alltså skett i enlighet med lag.[243] Även då man i tidigare domar kommit fram till att i ett område där missbruk potentiellt är så enkelt i enskilda fall, och kan ha så skadliga konsekvenser för samhället som helhet, det i princip är eftersträvansvärt att överlämna övervakningen över hur lagstiftningen sköts

[239] Kennedy v. England (application no. 26839/05) p. 130
[240] Ibid p. 153
[241] Ibid p. 154
[242] Ibid p. 155
[243] Ibid p. 155-170

till en domare, tycker man i det här fallet att det engelska systemet är tillräckligt.[244]

Då det finns tillräckliga skydd mot missbruk inbyggt i lagstiftningen, samt att IPT och kommissionären övervakar hur systemet sköts på ett generellt sätt, är åtgärderna tillåtna enligt artikel 8.2, det har följaktligen inte skett något brott mot konventionen. [245]

[244] Kennedy v. England (application no. 26839/05) p. 167
[245] Ibid p. 169-170

5 Vägar runt kryptering

För att komma till en slutsats rörande hur man kan komma runt kryptering, och få bilden klar över hur tekniken påverkar statens nuvarande tvångsmedel, kommer jag att ta upp tre möjliga vägar runt krypteringstekniken. Den första är metoderna från ett kriminalfall hämtat från verkligheten, den andra och tredje är lagstiftarens olika lagtekniska svar på utmaningarna från krypteringstekniken. Genom fallen kan man både dra slutsatser kring svagheterna och styrkorna kring krypteringstekniken.

5.1 Hunden i tunnan – Insatsstyrkan vs kryptering

Ett ännu ej slutligen avgjort kriminalfall[246] visar tydligt på både styrkorna och svagheterna hos krypteringstekniken. Polisen hade fattat misstankar mot en man som både misstänktes ha begått och dessutom planerade att snart utföra nya övergrepp på barn i utlandet. Mannen hade använt sig av en sorts krypterad kommunikation, men det fanns svagheter i den aktuella tekniken så att polisen trots detta kunde få fram hans identitet. Problemet i fallet var istället att man både visste att den information man behövde för att kunna få en fällande dom fanns i mannens dator, och att den misstänkte hade krypterat denna fullständigt. Problemet för polisen förvärrades dessutom av att den misstänkte också hade rigorösa säkerhetsrutiner för att undvika att någon skulle kunna komma åt datorn när den var igång och informationen därmed fanns tillgänglig utan lösenord; varje gång han avlägsnade sig från datorn, om så bara för att ta ett glas vatten, stängde han ned datorn. Vid en husrannsakan skulle det alltså inte finnas någon möjlighet för polisen att få tag i informationen, den misstänkte skulle hinna bryta strömmen så fort han hörde det minsta ljud, och alla bevis skulle i praktiken gå förlorade för utredningen.

För att försöka lösa situationen tog poliserna hjälp av nationella insatsstyrkan. Insatsledaren där utarbetade en plan för att trots allt försöka komma åt datorn under tiden som den användes av den misstänkte, utan att han skulle hinna stänga ned den. Planen gick ut på att insatsstyrkan tränade en stor polishund så att denna på kommando skulle söka sig mot en sittande person och hoppa upp i dennes knä, hunden kunde dessutom snabbt skjutas in i lägenheten i en slags cylinder.

Vid tiden för insatsen apterade insatsstyrkan först sprängladdningar på flera fönster, ögonblicket efter att dessa detonerade sköts hunden in i lägenheten, och hoppade omedelbart upp på den misstänkte när han satt vid datorn.

[246] Hela referatet av fallet bygger på telefonkontakt den 30 december 2013 med Björn Sellström, chef för Rikskriminalpolisens grupp mot sexuella övergrepp på barn och barnpornografi.

Försatt i fullständigt chocktillstånd av stora explosioner, ljudet av krossat glas och att plötsligt ha en stor hund i knäet hann den misstänkte inte bryta strömmen till sin dator innan insatsstyrkan kunde rusa in i lägenheten, gripa honom och säkra bevisningen.

5.2 Hemlig dataavläsning – Ett nytt tvångsmedel

SOU 2005:38 behandlar bland annat hemlig dataavläsning. Man konstaterar redan i inledningen att det förts fram från både åklagare och polis att det behövs ett nytt tvångsmedel i Sverige, liknande det som kallas dataavläsning och finns i Danmark. Man konstaterar att metoden är laglig även i andra europeiska länder samt USA och Kanada. Kort sammanfattat innebär metoden att myndigheterna har möjlighet att få information om användandet av en dator samt dess innehåll.[247]

Man konstaterar att bakgrunden till dataavläsning är ”de mycket stora svårigheter som finns i brottsutredningar med krypterad information och liknande i datorer och det faktum att det är lätt att vara anonym vid användning av informationsteknik.”[248]

Datavläsning skulle kunna innebära att man i hemlighet sänder ett program till en dator, sedan kan detta ge myndigheterna information om vad som finns i datorn och hur denna används. Dessutom kan myndigheterna läsa av informationen innan den förs över trådbunden eller trådlös kommunikation. Dataavläsning kan även innebära att man installerar hårdvara i datorn vid ett hemligt ingrepp, exempelvis genom att hemligen ta sig in i en persons bostad. Myndigheterna kan i viss mån välja vilken information som ska lagras eller sändas till myndigheterna, och därmed precisera den. De kan även välja om informationen skall skickas till dem eller lagras i datorn för beslag längre fram i tiden.[249]

Rörande frågan om metoden är effektiv, och om det finns ett påtagligt behov av den, konstaterar man att reglerna om hemlig teleövervakning och hemlig teleavlyssning funnits under lång tid, och att teknikutvecklingen under tiden varit oerhört kraftfull och dessutom skett mycket snabb. Man anser det självklart att de senaste nyheterna på teknikområdet används i särskilt grov brottslighet. Man anser det därför helt nödvändigt för samhället att myndigheterna inte hamnar hopplöst efter, utan inom ramen för ett rimligt integritetsintrång får möjlighet att använda effektiva metoder som är anpassade till den tekniska situationen vid varje uppkommet läge.[250]

[247] SOU 2005:38 s. 348
[248] Ibid s. 361
[249] Ibid s. 361
[250] Ibid s. 362

Man anser att frågan om dataavläsning måste ses i skenet av den pågående tekniska utvecklingen, och de kriminellas förmåga att hela tiden ligga i framkant och använda sig av allt säkrare former för kommunikation.[250]

Särskilt vid brottslighet som är av organiserad eller i övrigt allvarlig art, är ofta vissa av deltagarna oerhört skickliga i användandet av datorer. Man anser att de utnyttjar alla sina färdigheter för att med hjälp av datorerna dölja information, se till att vara anonyma och därmed undgå upptäckt.[250]

Utredningen konstaterar att teknikutvecklingen lett till att det nuförtiden finns stora problem i brottsutredningar när det kommer till att få fram information ur datorer, eller avlyssna information som sänds mellan datorer. Detta är något som är särskilt påtagligt när informationen är skyddad med kryptering. I allt fler brottsutredningar påträffar man information som är krypterad.[250]

Man diskuterar den allt mer omfattande användningen av kryptering, det ökande programutbudet och tillhandahållare av kommunikationstjänster som ger kunden möjlighet till kryptering för att få komplett informationssäkerhet. Det finns hos allmänheten en kraftigt ökande kunskap om lösningar för att skydda sig mot insyn genom bland annat program för att kryptera information. Man säger att många företag ser kryptering som nödvändigt i konkurrenshänseende.[251]

Utredningen konstaterar vidare att för att myndigheterna ska ha en möjlighet att få tillgång till den annars krypterade informationen krävs att den också existerar i klartext eller att myndigheten får tillgång antingen till datorn när krypteringen är upplåst eller till det hemliga lösenordet som kan låsa upp informationen. Man konstaterar dock att detta i dagsläget är ytterst ovanligt.[252]

Man anser att det vid tiden för utredningen är ovanligt att de brottsbekämpande myndigheterna får tillgång till information som finns i datorer när det gäller utredningar rörande kvalificerad brottslighet. Man säger att hemlig dataavläsning skulle göra det betydligt lättare för myndigheterna att komma runt problemet med krypterad information och ospårbara kontakter.[253]

Det uttalas också att hemlig teleavlyssning inte kan användas för att komma runt kryptering, utan bara fångar upp de krypterade meddelandena. För att få tillgång till den okrypterade informationen behöver den fångas upp redan i den anordning som personen använder.[253]

Man konstaterar också att det är ett allvarligt problem att människor kan agera anonymt vid användandet av informationsteknik**.** Avsaknaden av en skäligen misstänkt person är vanligtvis utgångsläget vid utredande av

[251] SOU 2005:38 s. 363
[252] Ibid s. 363-364
[253] Ibid s. 364

internetrelaterade brott. Även om det är möjligt för myndigheterna att knyta ett agerande på nätet till en viss IP-adress, och därefter via internetoperatören få reda på vems abonnemang som kan knytas till adressen vid en viss tidpunkt, säger det dock inget säkert om vem som egentligen satt vid datorn vid den tidpunkten. Man menar att en användning av dataavläsning då skulle innebära att man trots allt kan identifiera personen genom andra aktiviteter på internet.[254]

Man konstaterar avslutningsvis att det knappt finns några alternativa sätt att få fram den gömda informationen på än genom hemlig dataavläsning.[255]

Man tar upp flera fall där man hittat krypterad information, bl.a. i samband med Göteborgskravallerna, då i den s.k. sambandscentralen, samt vid ett fall rörande narkotikaförsäljning.[256]

Man framhåller att metoden med hemlig dataavläsning kräver en del förberedande åtgärder, och därför troligen bara skulle användas i fall där myndigheterna är övertygade om att metoden skulle resultera i viktig information.[257]

Rörande risken att verkställigheten röjs, går man inte in på det utöver att man fått röjningsriskerna beskrivna, samt sätt att reducera risken. Man går inte in på det djupare pga. sekretesskäl, av samma skäl går man heller inte in på effektiviteten av tvångsmedlet beroende på om det genomförs genom användning av hård eller mjukvara.[258]

Integritet

Man konstaterar att det finns ett stort behov av hemlig dataavläsning och att metoden framstår som effektiv, och att det då kvarstår att se om metoden kan motiveras utifrån integritetssynpunkt.[259]

Som jag tidigare nämnt tar man då upp att det är svårt att väga integritetsintressen mot nödvändigheten av att myndigheterna effektivt kan utreda brott.[260]

Man anser att de tvångsmedel som är allvarligast utifrån integritetssynpunkt är hemlig teleavlyssning och hemlig kameraövervakning. Man anser det svårt att avgöra hur stort intrång hemlig dataavläsning kan innebära, men anser att den i alla fall inte kan bli värre än hemlig teleavlyssning och kameraövervakning, som innefattar en mer total kontroll av och insyn i en pesons privatliv än vad dataavläsning gör. Det finns också en större risk att

[254] SOU 2005:38 s. 364
[255] Ibid s. 365-369
[256] Ibid s. 365
[257] Ibid s. 366
[258] Ibid s. 366
[259] Ibid s. 367
[260] Ibid s. 367

ovidkommande personer avlyssnas, som t.ex. ringer den misstänkte.[261]

Man tillägger dock att flera tvångsmedel mot samma person självklart gör att integritetsintrånget ökar markant.[262]

I förslaget vill man att ett godkännande av hemlig dataavläsning skall beslutas av domstol. Ett offentligt ombud skall liksom vid exempelvis hemlig teleavlyssning medverka vid domstolsförhandlingen.[263]

Man anser att tvångsmedlet skall kunna användas dels för brott där det inte är föreskrivet lindrigare straff än fängelse i två år samt försök, förberedelse och stämpling till sådant brott, dels bland annat hets mot folkgrupp, dataintrång och barnpornografibrott. Tvångsmedlet skall även kunna användas vid annat brott om dess straffvärde kan antas överstiga två år.[264]

5.2.1 Teoretiska användningsmöjligheter

Då man inte närmre diskuterar hur effektivt tvångsmedlet skulle kunna tänkas bli när det gäller alternativen hård/mjukvara, är det svårt att veta hur man skulle kunna tänkas använda tvångsmedlet.

Beroende på hur det skulle kunna tänkas fungera, kan det integritetsintrång det medför vara större eller mindre. Återkopplar man till fallet med hunden, ser man ett tydligt användningsområde för tvångsmedlet – istället för den dyra insatsen med hunden hade man kunnat låta en tekniker snabbt installera en apparat i exempelvis tangentbordet till datorn, som registrerade knapptryckningarna. Därefter hade man kunnat göra en normal husrannsakan och både fått med sig den krypterade datorn och lösenordet när den misstänkte väl knappat in det en gång.

I utredningen diskuterar man möjligheten för åklagaren att själv kunna förordna om hemlig dataavläsning, då "ibland kan det enda sättet att använda tvångsmedlet vara att sända en mjukvara till en dator när personen använder internet. Det kan tex. vara oklart var datorn rent fysiskt befinner sig eller så är ett hemligt intrång inte möjligt av andra skäl."[265] Man är dock inte beredd att föreslå något sådant innan bestämmelsen har tillämpats en tid, för att se om det finns ett behov av en sådan möjlighet.[266]

Även här kan man tänka sig fallet med hunden. Om man inte hade vetat vilken adress den misstänkte hade, eller inte kunnat genombryta en anonymitetstjänst, hade det kanske varit möjligt att istället sända över ett datorvirus till datorn som hade kunnat ta reda på de nödvändiga uppgifterna. Att en sådan möjlighet finns kan ha varit en av anledningarna till de rigorösa

[261] SOU 2005:38 s. 367-368
[262] Ibid s. 368
[263] Ibid s. 372
[264] Ibid s. 373
[265] Ibid s. 372
[266] Ibid s. 372-373

säkerhetsrutiner som The Guardian vidtog när det kom till materialet från Edward Snowden. Man köpte in särskilda datorer, som förseddes med tredubbla lösenord, dessa fick aldrig kopplas upp mot internet. Datorerna fick stå i ett rum med förtäckta fönster som vaktades av inhyrda väktare.[267]

Så långt liknar tvångsmedlet andra metoder såsom hemlig telefonavlyssning, med den oerhört viktiga skillnaden att det dessutom blir möjligt att avslöja identiteten hos en person som använder sig av en anonymitetstjänst.

En annan viktig aspekt är dock de frågor som väcks i anslutning till att tvångsmedlet skall kunna användas vid brottet hets mot folkgrupp. Frågan blev ytterst aktuell i spåren efter Breiviks terrorattack i Norge, och resulterade bland annat i att kommentarsfält till tidningsartiklar på nätet stängdes ned.[268] Även om jag inte har någon statistik i ämnet, tror jag det kan sägas vara allmänt veterligt att den största andelen brott mot lagen om hets mot folkgrupp begås på internet, nämligen i kommentarsfält till nyhetsartiklar, blogginlägg, "alternativ media", och slutligen givetvis forumet Flashback.

Om lagstiftningen skall kunna vara effektiv, vilket man anser den bli i utredningen, måste den kunna vara effektiv även för att komma åt den här typen av brottslighet. En möjlig lösning för att komma åt människor på exempelvis Flashback skulle då vara att infektera hela webbsidan med ett verktyg för hemlig dataavläsning, som är inställt på att angripa personer med användarnamn som man fått domstolsbeslut för verkställande av tvångsmedlet på.

På det viset skulle tvångsmedlet kunna ha en god effekt för att få tag på de anonyma personerna bakom användarnamnen, oavsett om de dessutom använder en anonymitetstjänst. Den möjligheten väcker en mängd frågor, som jag kommer att diskutera närmre i min analys.

Man får en rätt bra bild av hur den mjukvarubaserade delen av tvångsmedlet skulle kunna fungera om man tittar på den diskussion som uppstod i Tyskland, efter att en hackergrupp upptäckt en ”stats-trojan”[269] efter ett anonymt tips. Trojanen hade förmåga att ta närmast total kontroll över den dator den infekterade. Hackergruppen hävdade även att skyddet runt trojanen var så svagt att den skulle kunna användas av helt andra parter.[270]

Det har höjts flera röster om tvångsmedlet. Både advokatsamfundet och datainspektionen ställde sig negativa till införandet av olika skäl. Advokatsamfundet främst då många frågor rörande den personliga

[267] http://www.sydsvenskan.se/kultur--nojen/storyn-med-stort-s--ett-besok-hos-the-guardian/
[268] http://www.dn.se/kultur-noje/sa-hanterar-svenska-tidningar-nathatet/
[269] ”Trojan” är en beteckning för en viss typ av datorvirus
[270] http://www.dw.de/several-german-states-admit-to-use-of-controversial-spy-software/a-15449054-1

integriteten var obesvarade, exempelvis hur man ska se på möjligheterna att genom hemlig dataavläsning använda en dator utrustad med mikrofon och webbkamera för att uppnå samma resultat som vid buggning. Man anser det också orimligt att dataavläsning, som skulle kunna användas för att avlyssna internettelefoni, skulle få användas vid brott med så låg straffskala att inte ens teleövervakning fått äga rum innan då nyligen genomförda författningsändringar. Man anser istället att hemlig dataavläsning skulle få längre gående följder än hemlig teleavlyssning.[271] Datainspektionen riktar precis som advokatsamfundet in sig på frågan om att både ljud, bild och privat korrespondens kan hämtas in via tvångsmedlet, som man därför anser vara mer integritetskränkande än andra befintliga tvångsmedel.[272] Man framhåller också att man inte har förutsättningar att bedöma behovet av tvångsmedlet, enligt kraven i bland annat Europakonventionen.

Det lyftes även fram rent teknisk kritik mot tvångsmedlet från annat håll. Forskningschefen för det norska datasäkerhetsföretaget Norman hävdade dels att det redan fanns program som gjorde att försök att använda tvångsmedlet troligtvis skulle upptäckas, dels vände han sig starkt emot tanken på att datasäkerhetsföretag i så fall kanske skulle tvingas bygga in bakdörrar i sina program så att tvångsmedlet skulle kunna användas ändå.[273]

Tvångsmedlet infördes aldrig. SOU 2005:38 behandlades senare i en proposition, dock utan att det föreslogs ett införande av delen om hemlig dataavläsning.[274]

Tvångsmedlet efterfrågas dock fortfarande. Ekobrottsmyndigheten efterfrågade senast i slutet av 2012 en utredning rörande ytterligare hemliga tvångsmedel med hänvisning till kryptering och den tekniska utvecklingen, och nämnde då att man tidigare ställt sig positiv till hemlig dataavläsning.[275]

5.3 Dekryptering under straffhot

Jag tänker här återkoppla till min tidigare uppsats, och de resultat jag kom fram till där.

1. Sammanfattning av min tidigare uppsats

I min tidigare uppsats, "Kryptering, dekryptering och de mänskliga rättigheterna", valde jag att undersöka en aspekt av krypteringstekniken, nämligen problematiken kring information som krypterats så att enda möjligheten att komma åt den är att få den misstänkte att avslöja lösenordet. Jag kommer mycket kort referera min uppsats och de slutsatser jag kom fram till i det här arbetet, för en mer ingående analys hänvisar jag till mitt

[271]Dnr: R-2005/1309, Remissyttrande Sveriges Advokatsamfund, 2005 s. 2-3
[272] Dnr: 1391-2005, Remissyttrande Datainspektionen, 2005, s. 5
[273]http://www.realtid.se/ArticlePages/200609/22/20060922082335_Realtid597/20060922082335_Realtid597.dbp.asp
[274] Proposition 2011/12:55 s. 1-2
[275]Dnr: EBM A-2012/0363, Remissyttrande Ekobrottsmyndigheten, 2012, s. 5

ursprungliga arbete, som finns enkelt tillgängligt på internet.[276] Här nedan följer därför först en kort genomgång av de mest relevanta delarna av mitt arbete, därefter följer en kort uppföljning av hur det ser ut på rättsområdet idag.

Den engelska lagstiftning som införts som en reaktion mot krypteringstekniken gick i korthet ut på att den misstänkte, under vissa förutsättningar, under straffhot kunde tvingades uppge lösenordet till krypterad information.[277]

Jag valde att undersöka lagstiftningen i förhållande till Europadomstolens rättspraxis om rätten till en rättvis rättegång, för att se om det skulle vara möjligt att införa liknande lagstiftning i Sverige, jag analyserade även hur de engelska domstolarna resonerat om lagstiftningens förenlighet med Europakonventionen.

Från Europadomstolen var tre fall aktuella. I fallet Funke v. Frankrike var en person misstänkt för skattebrott, efter en husrannsakan för att inhämta handlingar om tillgångar i utlandet hade man inte nog med information, utan bad den misstänkte att inkomma med ytterligare handlingar, denna begäran kunde sanktioneras med böter eller fängelse. Europadomstolen kom fram till att då man bett den misstänkte att ta fram handlingar man själv inte kunnat hitta, hade man gjort sig skyldig till ett brott mot artikel 6. Inte heller tullrättens speciella karaktär kunde motivera en inskränkning av artikeln. Man gick på den klagandes linje.[278]

I fallet Saunders v. The United Kingdom rörde det sig om en komplicerad insideraffär i ett stort företag. Under utredningen använde sig staten av särskilda inspektörer, dessa hade befogenheten att begära ut olika typer av handlingar, och de anställda var även i övrigt tvungna att bistå utredningen. Att inte lyda inspektörerna var ett brott som kunde leda till fängelse, och den information som man lämnade kunde användas emot en i en kommande rättegång, vilket skedde mot den klagande i fallet. Europadomstolen kom fram till att rätten att inte behöva vittna mot sig själv hade blivit kränkt, och att denna generellt sett dessutom utgör själva kärnan i artikel 6. Man gick på den klagandes linje även här.[279]

Det sista fallet jag analyserade, Heany and McGuiness v. Ireland, rörde terrorism. Två män hade blivit gripna misstänkta för att tillhöra IRA, efter en terrorattack som krävt 6 människoliv. Enligt irländsk lagstiftning kunde man under straffhot kräva att de redogjorde för var de befunnit sig under attentatet. De klagande vägrade, vilket resulterade i ett fängelsestraff. Även här gick Europadomstolen på de klagandes linje, och ansåg att inte heller terrorbekämpning kunde motivera en inskränkning i artikel 6. I fallet förtydligade man också att rätten till tystnad inte är absolut, men att det

[276] http://www.lu.se/lup/publication/3046392
[277] Ibid s. 15
[278] Ibid s. 10
[279] Ibid s. 10-12

undantaget är något som kan aktualiseras i fall där den misstänkte blir upplyst om att hans tystnad kan tolkas som något negativt för honom när det finns annan bevisning mot honom. Då den irländska lagstiftningen istället satte den misstänkte i en situation där han fick välja mellan att tiga eller att straffas, blev Irland fällt.[280]

Slutligen gick jag igenom två domar från de nationella domstolarna, där dekrypteringslagstiftningen prövades mot Europakonventionen. Man kom fram till att ett föreläggande enligt den inhemska lagen ej stred mot rätten till tystnad, då själva krypteringsnyckeln oavsett innehållet i datorn var neutral, på samma sätt som nyckeln till en låst byrålåda, och inte i sig var ett erkännande av skuld. Man ansåg också att nyckeln existerande "oberoende av den misstänktes vilja", och därmed skulle falla in under samma regler som alkoholtester etc.[281]

Det man ansåg kunde vara komprometterande var däremot själva kopplingen mellan den misstänkte och kunskapen om hur man låste upp den krypterade informationen. Detta kunde nämligen koppla den misstänkte till denna. Då domaren kunde utesluta den delen av bevisningen i rättegången, var detta dock ej något problem.[282]

Min slutsats rörande den engelska lagstiftningen blev att den stred mot Europakonventionen. Detta är en tolkning jag alltjämt vidhåller. Jag baserade detta, kort sammanfattat, på Europadomstolens praxis som entydigt verkade visa att den misstänkte inte ska tvingas hjälpa staten att få fram bevis mot sig själv. Blodprov, DNA och alkoholtester kan genomföras mot den misstänktes vilja, och informationen måste sägas existera oavsett den misstänktes vilja. En krypteringsnyckel däremot kan inte sägas existera oberoende av den misstänktes vilja, mer än ett erkännande av hur ett mord gick till. Det visar sig klart om man tänker sig en hypotetisk framtid där staten kan läsa av information i människors hjärnor, på samma sätt som man kan läsa av information i DNA eller alkohol i utandningsluft. Då krävs inte att den misstänkte samarbetar, utan informationen om krypteringsnyckeln existerar oberoende av den misstänktes vilja. Först under de hypotetiska förhållandena hade den engelska domstolens resonemang varit hållbart.[283] Jag argumenterade även för att den engelska lagstiftningen inte var effektiv, då de som hade krypterat information som, om den upptäcktes, kunde leda till stränga straff, också skulle vara de som vägrade uppge lösenordet.[284]

2. Vad har hänt sedan min tidigare uppsats?

Vad jag har sett har det inte skett några dramatiska förändringar på området. Den engelska lagstiftningen finns kvar, och systemet används relativt frekvent. Mellan 2012 och 2013 lämnades 26 ”dekrypteringsordrar” ut. I tre

[280] http://www.lu.se/lup/publication/3046392s. 12-14
[281] Ibid s. 18
[282] Ibid s. 18
[283] Ibid s. 21 - 25
[284] Ibid s. 20

av fallen lämnades nyckeln över, i nitton fall gjordes inte detta. Resterande fall var vid tiden för rapporten ej avslutade.[285]

I SOU 2013 tog man i samband med föreslagen lagstiftning för att bland annat tvingas lämna ut krypteringsnycklar[286] även upp att den misstänkte inte själv skulle vara tvungen att lämna ut sådan information, något som pekar på att lagstiftaren är av samma åsikt som mig.[287]

Nyligen lämnades en motion som delvis berör frågan in till riksdagen.[288] Riksdagsledamoten vill att företag som skapar krypteringsverkyg ska kunna tvingas att lämna ut krypteringsnycklar om förundersökningsledaren begär detta. Tyvärr är det en så pass ny motion att den inte kommer att hinna besvaras innan deadline för uppsatsen.

Min tolkning av motionen är att riksdagsledamoten tycks efterfråga ett system liknande ”key escrow”, ett system där en tredje part har kopior av en användares krypteringsnycklar,[289] dock i tron att företagen som tillverkar krypteringsprogram redan idag har någon typ av ”huvudnyckel” till programmen. Tanken är inte ny, USA försökte under 90-talet genomdriva liknande förslag genom OECD, dock utan framgång.[290]

[285] Office of Surveillance Commissioners, Annual Report 2012-2013 s. 12
[286] SOU 2013:39 s. 280-281
[287] Ibid s. 281
[288] Motion 2013/14:Ju277
[289] http://technet.microsoft.com/en-us/library/cc961626.aspx
[290] Black, Sharon, Telecommunications Law in the Internet Age, USA, 2002, s. 368-369

6 ANALYS

Frågeställningarna rörande hemlig dataavläsning:
– Vad hände med förslaget?
– Är det förenligt med Europakonventionen?
– Bör det enligt mig vara förenligt med Europakonventionen om man ser på domstolens tidigare praxis?
– Vad säger man inom olika myndigheter om kryptering? Vad säger exempelvis åklagare och poliser om dagens svårigheter och möjligheterna till nya tvångsmedel?

Jag ser inget direkt hinder mot varför förslaget om hemlig dataavläsning inte skulle vara förenlig med Europadomstolens praxis, även om det aldrig infördes i svensk rätt trots att både poliser och åklagare önskat en möjlighet att ta sig runt kryptering med hänvisning till svårigheterna den medför, och även i ett fall direkt efterfrågat hemlig dataavläsning. Jämfört med den engelska lagstiftningen för telefonavlyssning kan det svenska systemet användas även vid mindre allvarliga brott, men ser man på tendensen i Europadomstolens praxis bör inte detta vara ett problem, särskilt som lagstiftningen ytterst syftar till att komma åt allvarlig brottslighet.

Jag tror därför inte att den kritik som datainspektionen och Advokatsamfundet framför om tvångsmedlets inverkan på den personliga integriteten är skäl som skulle göra att tvångsmedlet inte accepterades av Europadomstolen. Det kriterium som Europadomstolen verkar ta mest fasta på, att en domare övervakar användandet av tvångsmedlet, var uppfyllt i utredningen.

Tvärtom tycker jag mig i min uppsats ha sett att hemlig dataavläsning snarare kommer att indirekt krävas än förbjudas, och detta blir tydligt när man ser på den moderna krypteringsteknikens oerhörda påverkan på nuvarande tvångsmedel, och hur man från både polis och åklagarhåll efterfrågat vägar runt olika typer av kryptering.

För att lagstiftning inte ska stå i strid med artikel 8 krävs det nämligen att den är effektiv för sitt syfte, att den korresponderar till behovet. Om man tittar på Europadomstolens tidigare praxis är det tydligt att staterna haft fog för sin uppfattning att exempelvis hemlig teleavlyssning är ett effektivt vapen i kampen mot grov brottslighet, men idag när krypteringstekniken används allt mer, kan detta onekligen börja diskuteras. I inledningen nämnde jag att det talades om en exponentiell ökning av antalet brottslingar som använder sig av krypteringsteknik, och med tanke på omständigheterna låter detta knappast orimligt.

Om vi inom en snar framtid ställs mot faktumet att en stor del av alla brottslingar av rutin använder sig av krypterad kommunikation, på samma

sätt som de idag använder sig av anonyma kontantkort, så borde det unika inträffa att det gamla tvångsmedlet hemlig telefonavlyssning faller på kriteriet effektivitet, det kan inte längre användas mot de företeelser som förut motiverade inskränkningen enligt artikel 8. Rimligtvis måste detta klassiska tvångsmedel i konsekvens med Europadomstolens egen praxis då förbjudas.

Dilemmat i Europadomstolens praxis är att staten har en utväg för att undvika detta, nämligen att se till att tvångsmedlet förblir effektivt, i det här fallet exempelvis genom att införa hemlig dataavläsning som ett komplement. Å ena sidan är effektivitetskravet alltså en garant för att staten inte inför integritetskränkande lagstiftning som inte kan användas mot de problem man anför som skäl för införandet, å andra sidan är det en faktor som är drivande mot ett samhälle där varje möjlighet till helt hemlig och förtrolig kommunikation en efter en måste avskäras i en stat som vill ha kvar sina klassiska möjligheter till hemlig avlyssning av kommunikation.

Draget till sin spets kan man se tre vägar, en där möjligheterna till anonym och säker kommunikation helt utplånas, en där staten tvingas ge upp vissa av sina klassiska befogenheter och således tvingas kapitulera inför tekniken, samt en där staten lämnar Europakonventionen för att fortsätta som tidigare, trots bristerna i effektivitet. Att politiker hotar med att lämna Europakonventionen har tidigare förekommit, exempelvis i England.[291] Båda de senare alternativen vore onekligen oerhört uppseendeväckande, och jag är övertygad om att Europadomstolen ogärna skulle vilja fatta ett avgörande som ställer staterna inför det vägvalet. Detta skulle kunna vara en anledning till, den i mitt tycke, anmärkningsvärda förändringen i synen på hemlig telefonavlyssning som följden av rättsfall från Klass till och med Kennedy ger uttryck för. Jag får personligen känslan av att Europadomstolen varit oerhört tillmötesgående gentemot staterna.

Något som nämligen tydligt framträder i Europadomstolens praxis, är att man från att ha sett hemlig telefonavlyssning och liknande åtgärder som något som fick förekomma i extremfall för att skydda nationen från spionerі och terrorism, och som även då måste omgärdas av ett effektivt skydd mot missbruk, gått över till en helt annan tolkningsmodell. Jag tolkar fallet Klass som att två rekvisit behövde uppfyllas för att domstolen skulle godkänna Tysklands lagstiftning. Dels behövde det finnas ett reellt behov av tvångsmedlet som uppväger den skada det potentiellt kan orsaka på demokratin. I fallet Klass ställdes då manuell telefonavlyssning och öppnande av brev mot hotet från terrorism och (troligen) spionerі från Sovjetunionen under kalla kriget, och statens intresse ansågs slutligen trots allt väga tyngst i kampen mot bland annat ”subversive elements”. Först därefter tittade man på vilka skydd mot missbruk lagstiftningen tillhandahöll, och om dessa var tillräckliga.

I senare avgöranden verkar det istället bara vara själva skydden mot

[291] http://www.bbc.co.uk/news/uk-politics-21726612

missbruk man tittar på. Omgärdas lagstiftningen av tillräckliga skydd mot missbruk, spelar det i praktiken ingen roll vilka brott den kan användas på, eller vilket potentiellt hot mot demokratin den utgör. Det engelska systemet där det var tillräckligt att brottet involverar våld, resulterar i en substantiell ekonomisk vinst, eller begås av en stor grupp människor för ett gemensamt mål torde, i teorin, kunna inrymma stora delar av strafflagstiftningen i en stat. I det sista rekvisitet skulle man kunna tänka sig att fredliga aktioner, som Greenpeaces aktioner mot kärnkraftverk, blockader av affärer etc. skulle kunna räknas in.

Europadomstolen verkar helt ha släppt tanken på att lagstiftningen i sig kan utgöra ett hot mot det demokratiska samhället, att den bara i en situation med överskuggande hot från spioner och terrorister kunde tillåtas. Istället banar man nu väg för ett samhälle av utökad statlig kontroll, där utbyggnaden av ett totalt övervakningssystem, förvisso helst kontrollerat av domare, bit för bit kan byggas upp, förment helt i enlighet med Europakonventionen.

Detta är en oerhört anmärkningsvärd praxisförändring, och torde inte stämma väl överens med intentionerna bakom det ursprungliga fallet Klass. Istället bör det, som domare Petitti gick in på, vara så att framväxandet av den moderna tekniken ställer frågan i ett nytt ljus och gör att man tvingas omvärdera synen på övervakning åt ett motsatt, mer restriktivt, håll.

Det system i Klass, som måste ha skötts relativt manuellt (och riktade in sig mot ”subversive elements”), får antagligen sägas vara väsenskilt från dagens system inbegripande big data, som helt automatiserat utifrån sökbegrepp kan inhämta oerhörda mängder privat information ur konversationer och processa dessa helt automatiskt, och tillsammans med alltifrån kontakter och läsvanor till gps-postioner skapa profiler över enskildas personer. Något sådant var helt enkelt inte tekniskt möjligt vid tiden för Klass.
Det får även sägas vara väsenskilt från det system domare Pettitti såg som så modernt, tekniken har som bekant kommit fruktansvärt långt sedan 1984 då det fallet avgjordes.

En enligt mig rimligare tolkning av fallet Klass hade varit att det ställs allt högre krav på skälen för en åtgärd som inskränker artikel 8, allteftersom tekniken utvecklas så att den potentiella skadan den kan orsaka på demokratin växer. Att ha möjligheten att manuellt avlyssna enskildas kommunikation är en sak. Att bana vägen för ett system som ger staten en teoretisk möjlighet att med automatik klassificera individer efter deras åsikter, genom att avlyssna och samköra i princip all kommunikation är något helt annat. Idag, när staterna förfogar över allt större datorresurser och det av både statliga och privata aktörer skapas enorma register som potentiellt kan samköras, bör Europadomstolen sätta ned foten och konstatera att det första rekvisitet inte längre är uppfyllt, nu väger istället vågskålen över till fördel för den enskilde, och existensen av systemen i sig är för farliga ur demokratisynpunkt.

I nuläget ser det dock som sagt inte ut att finnas någon sådan tendens hos domstolen, utan jag ser inget hinder mot att hemlig dataavläsning skulle kunna införas utan att lagstiftningen skulle fällas av Europadomstolen.

Vilken syn på integritet och anonymitet är allmänt rådande idag? Vilka konkurrerande teorier finns det på området?

Genom mitt arbete tycker jag mig ha hittat tre olika teorier rörande den personliga integritetens ställning i förhållande till kampen mot olika typer av brottslighet.

– Den första teorin, som bl.a. Tännsjö ansluter sig till, går ut på att integritet och anonymitet i princip ska tillåtas helt försvinna. Men även andra, som man inte kunde ha förväntat sig, som en chefredaktör på en tidning, är emot möjligheten till att vara anonym på internet.

– Den andra teorin, mellanlösningen, är den som till stor del används idag, och nog får sägas vara den allmänt rådande. Den går ut på att staten har rätt att se i princip all information om det är för att tillvarata ett angeläget intresse, så länge den enskilde individens rättigheter skyddas av en domstol. Domaren utgör garanten för att ett övervakningssystem inte missbrukas, och Europadomstolens praxis går som sagt att tolka som att i princip vilken form av övervakning som helst går att acceptera, så länge en domstol övervakar användandet och tvångsmedlet anses behövas för den nationella säkerheten. Under sådana förhållanden skulle den nämligen alltid anses vara proportionell.

I den här teorin är möjligheten till helt anonym kommunikation något som inte kan tillåtas, av skilda skäl. Detta blir tydligt när man läser uttalandena i SOU 2005:38, tittar på debatterna kring anoymitetstjänster, tolkar Europadomstolens avgöranden eller ser hur meddelarskyddet i tryckfrihetsförordningen är uppbyggt. Att staten kan sanktionera en viss anonymitet är en sak, att staten defacto skulle stå utan möjlighet att ingripa mot upphovsmannen eller förmedlaren av viss information eller kommunikation är en helt annan sak.

– Den tredje teorin om integritet i förhållande till övervakning är splittrad, och utgörs av författare från skilda läger, Anne-Marie Eklund-Löwinder på toppdomänstiftelsen .SE, i viss mån staten genom agerandet för att stödja TOR via SIDA, Piratpartiet, och forskarna som replikerade på Tännsjös artikel.

Den stora, och avgörande, skillnaden här ligger i stödet för möjligheten att agera anonymt på internet och i elektronisk kommunikation med andra människor. Istället för att se krypteringstekniken som ett hinder för brottsutredande myndigheter, väljer man att se den som något positivt som ger individen möjlighet till en skyddad sfär gentemot staten. Här ser man det som någonting positivt att staten inte alltid har möjlighet att få tag i all information, och vill se till att den möjligheten fortsatt skyddas.

Vilken teori anser jag är rimlig att använda när det gäller tvångsmedel i förhållande till kryptering? Av vilka skäl?

Jag personligen anser att det bör vara den tredje teorin som bör vara rådande i arbetet med att stifta ny lag. Jag baserar den åsikten på flera olika anledningar, där den första är farorna med ett alltför utbyggt övervakningssystem. Neil M. Richards berör detta på ett bra sätt i sin artikel, men han undviker att dra resonemanget till sin självklara spets. Efter att ha pekat på alla faror med övervakning, och gått in på samma resonemang som domare Petitti, så väjer han för problemet genom att vilja förbjuda total övervakning, men fortfarande vara öppen för övrig övervakning som en domstol beslutar om. Både Petitti och Neil hamnar alltså i ”domaren som universallösning mot missbruk”, och en tro på att lagstiftaren inte bygger upp ett system som senare plötsligt kan missbrukas av en ny regim, eller någon annan.

Jag är istället av åsikten att de *blotta möjligheterna* till hemlig övervakning blir allt allvarligare integritetsmässigt ju mer övervakningstekniken förfinas och vi blir allt mer beroende av internet för att effektivt kunna inhämta information och uttrycka åsikter. Under tiden för fallet Klass talade man om ”the spectre of surveilance”, trots att det rörde sig om manuell avlyssning. I dag, när information automatiskt kan avlyssnas, filtreras och samköras på ett helt annat sätt, krävs andra metoder för att skydda den enskilde gentemot staten.

Vilken typ av sidor du besöker, vilka varor du köper, vilka kvarter du befinner dig i på vilka tider, vilka nyheter du läser, vilka sökord du skriver in på Google – all information går idag att samköra tillsammans med information om dina vänner, och en allt exaktare profil kan byggas upp. Det är ett allvarligt problem att den övervakning som hittills byggt upp och som motiverats för att vara mot grova brottslingar, enligt vad jag kommer fram till i min uppsats, visat sig i verkligheten vara tämligen ineffektiv. Det har hela tiden funnits vägar runt för dem som verkligen vill undgå övervakning. Istället är det de vanliga människorna, de som inte anser sig ha något att dölja, som teoretiskt är mest utsatta för övervakningen.

Jag tror det är ett okontroversiellt påstående att internet och den moderna kommunikationen skiljer sig stort från tidigare kommunikationsformer, i och med dess relativa anonymitet och möjlighet till snabb kommunikation. Det är bara att se på hur kinesiska dissidenter kan blogga kritiskt om regimen, hur Wikileaks blixtsnabbt kan läcka information, hur både The pirate bay och forumet Flashback vid tiden för min uppsats fortfarande existerar. Den fråga man bör ställa sig är om vi verkligen vill förändra detta i grunden?

Om man då närmre granskar argumentet med domaren som garant för att staten inte ska missbruka ett övervakningssystem, som framhålls som så starkt och slutligt båda av författare inom juridik och domarna i Europadomstolen till stöd för den andra teorin, framgår fyra tydliga

svagheter.

1. Det är relativt enkelt att stifta ny lag, samt påverka tolkningen av gammal lag, och domare har i ett historiskt perspektiv visat sig ha problem att stå emot en repressiv regi. Systemet kan dessutom oavsett missbrukas.

Det är bara att se på hur domare agerade i Tyskland under nazisttiden eller DDR, och hur snabbt man då anpassade sig till en ny ordning som vände upp och ned på alla begrepp.[292] Även om man inte går så långt att man förväntar sig det orimliga i att en diktatur skulle vara medlem i Europakonventionen, så är det inte lika långt bort att tänka sig ett system där man går för långt i kampen mot olika ideologiska rörelser, eller där man i ett krisläge som under andra världskriget, alternativt även under stark press från omvärlden[293], vill inskränka möjligheterna till spridandet av viss information.

Jag anser det också vara något oerhört problematiskt att staten skall vara den som bestämmer vilken väg som är den rätta, och får ett effektivt verktyg för att tysta och stoppa människor som anser något annat. Vad hade resultatet blivit om staten hade haft dagens möjligheter till övervakning tidigare i historien? Avlyssningen av Marthin Luther King grundades på att han var ett ”hot mot ordningen” i samhället. Idag ser vi det som att det var en självklar och viktig förändring som han genomdrev, men då sågs han istället bara som ett hot. På samma sätt kan man fråga sig vad som hänt om katolska kyrkan haft motsvarande övervakningsapparat vid tiden då Galileo levde? Vad hade hänt om Sovjet hade haft det? Vad hade hänt om kungamakten hade haft det under franska revolutionen? Ghadaffi? Om Sydafrika haft det i förhållande till Nelson Mandela?

Det engelska övervakningssystemet används som Neil skriver för att köra ut ungdomar ur stadskärnorna, och den engelska lagstiftningen för avlyssning kan användas mot ”flera personer som strävar efter ett gemensamt mål”. Det är som sagt enkelt att se hur ett sådant system skulle kunna användas för att i förtid stoppa olika, olagliga, aktioner som många dock anser bör kunna genomföras, och där deltagarna får sina straff i efterhand. Ett exempel skulle kunna vara Greenpeaces olika fredliga demonstrationer, där man som ett led i aktionen begår exempelvis olaga intrång.[294] En anledning till att det juridiska systemet har fungerat är troligen att det faktiskt går att bryta mot lagen, och sedan bli dömd, vilket kan göra att människor reagerar mot domen och kräver lagändringar. Att i tysthet kunna stoppa precis alla brott under planeringsstadiet, innan de hinner väcka uppmärksamhet, skulle enligt min mening faktiskt allvarligt kunna skada det juridiska systemet.

Om man tittar på exemplet med marknadsföringskedjan Target som Neil tar upp, bör det redan idag vara möjligt att med bra datorprogram kunna lyfta fram argument för eller emot olika politiska rörelser och ideologier, som

[292] Jmf. Modéer, Kjell, Juristernas nära förflutna, 2009 s. 269
[293] Jmf. http://www.svd.se/nyheter/inrikes/laila-freivalds-avgar_302444.svd
[294] Jmf. exempelvis http://www.dn.se/nyheter/sverige/greenpeace-inne-pa-karnkraftverk/

dyker upp som reklam på internet när de kan tänkas vara som mest effektiva. Genom ett sådant system hade det kanske inte behövts någon våldsam repressiv stat – efter en tid skulle det vara omöjligt att förankra nya idéer i de breda folklagren, eftersom information som bryter mot koncensus i samhället effektivt skulle argumenteras ned innan den fick fäste, i kombination med att upphovsmännen till den skulle kunna tystas eller stängas av från internet.

Det ligger ett uppenbart problem i att vi idag anser oss vara så högt stående över tidigare generationer att vi kan hantera möjligheten till övervakning och kontroll av den här graden, när man lätt ser hur absurt det vore att motivera den förr i tiden genom att hänvisa till en kamp mot brottslighet. Förändringarna som tidigare generationer slogs för bör väl objektivt sett trots allt ha vägt tyngre?

2. Systemet kan missbrukas av fler aktörer än staterna

Då övervakning idag inte längre framförallt handlar om att avlyssna enskilda personers telefonsamtal, utan om att automatiskt samla in och koppla ihop oerhörda mängder data, blir det allt mer sannolikt, precis som Neil tar upp, att det blir möjligt att staten har information om människor som kan användas för att enkelt och effektivt tysta dem. Det stora problemet är att det inte behöver krävas stora samhällsomvälvningar för att ett övervakningssystem ska kunna riktas mot dissidenter i samhället, utan det kan räcka med en person som Hoover, som relativt autonomt från staten agerar för vad han tycker är det rätta. Det ligger också i sakens natur att de på högst positioner i samhället kan ha mest att förlora på att information om dem röjs, och man kan lätt tänka sig att både domare och politiker kunde tvingas böja sig för ett sådant system när det väl satts igång, precis som man fick göra för Hoovers system.

Ett troligen större problem vore om storföretag och andra ekonomiska intressen kunde utnyttja och påverka vilken information som samlas in. Redan idag upplever nog de flesta att det är ett problem hur mycket storföretag kan påverka genom lobbying i EU. I en tid då staterna blir allt svagare gentemot globala storföretag, är det lätt att tänka sig en framtid där näringslivet kan nästla sig in i övervakningssystemet och utnyttja det för sina egna syften, som kan ligga ännu längre bort från folkets vilja än en diktators eller underrättelsechefs.

Till den klassiska faran om staten som missbrukar sin makt mot den enskilde, tillkommer då företag i ekvationen. Det är bara att titta på Doles agerande i processen mot filmen ”Bananas”, eller Scientologkyrkans påtryckningar för att stoppa information om kulten, för att se vilka andra intressen som skulle kunna vara intresserade av att utnyttja sig av lagstiftningens möjligheter. Även Expressenfallet och Ryanairfallet visar på farorna när en part vill kunna tysta ideologiska motståndare. Tanken att en ”politisk Snowden” röjer oerhörda mängder uppgifter som berör enskildas

privatsfär, och någon sedan publicerar dessa för att skrämma dem och andra till tystnad, känns inte längre avlägsen.

Slutligen resulterar detta, som Neil också var inne på, att man undviker att gå in och läsa eller skriva information eller befinna sig på platser som, om det upptäcktes, skulle kunna verka menligt på ens karriärmöjligheter. En kultur av självcensur skulle lätt kunna utvecklas.

Det sägs vara en regel att en marknadsekonomi genom konkurser och sammanslagningar av företag leder till allt färre aktörer, i en globaliserad ekonomi där enskilda företags ageranden kan få ett lands ekonomi på fall, bör det allvarligt ifrågasättas vilka tvångsmedel som ska få finnas "färdiga att använda" för staten i ett helt annat syfte än vad det var tänkt från början, där det enda skyddet för den enskilde utgörs av domare och skriven lag.

3. Det skapas lätt ett system där det blir svårt att ställa någon till svars

Beroende på om man ska tro att Obama talar sanning eller inte om att han inte kände till viktiga delar av den övervakning NSA sysslade med, skapas ett ytterligare argument mot domaren som garant för att ett övervakningssystem inte missbrukas. När ett underrättelsesystem väl är beslutat, finansierat och uppbyggt, kan det bli oerhört svårt att se hur det används. Man kan inte vara säker på att varken politiker eller domare verkligen informeras vad som pågår bakom slutna dörrar precis som i fallet med NSA.

4 *Det måste vara möjligt att bryta mot lagen*

Mitt sista argument, som jag delvis gick in på tidigare, är att det i vissa fall måste vara möjligt att bryta mot lagen. I en framtid där signalspaning är mer utbyggd, och där man kan koppla människor till politiska åsikter och ideologier kan man se till att inte potentiella terrorister får viktiga ämbeten, vare sig det är inom det militära eller det civila. Men ska ett sådant system fungera, får man anta att ett system som skulle kunna tända en varningslampa över Edward Snowden, eller Bradley Manning[295] på samma sätt skulle vara effektivt.

Hade en tillräckligt sofistikerad underrättelsetjänst genom att undersöka deras kontakter, internetanvändning, nyhetsläsning och samtal kunnat få fram deras politiska åsikter och ideal, och i god tid kunnat förflytta dem till arbeten med mindre tillgång till hemlig information? Kanske, beroende på omständigheterna!
Hade staten kunnat motivera ett övervakningsprogram[296] mot exempelvis "personer med tillgång till kritisk information som kan skada rikets

[295] Bradley Manning släppte som bekant tusentals sidor hemliga dokument, samt en video som visade hur amerikanska soldater besköt civila.
http://www.svd.se/nyheter/utrikes/bradley-manning-doms-till-35-ars-fangelse_8442090.svd
[296] I slutet på 70-talet ledde det faktum att en agent hos Säpo lagt märke till att snickaren Leander parkerat sin bil på en skolgård i samband med att där hölls ett möte för tidskriften

säkerhet" för att bekämpa spioneri, för att med hemlig dataavläsning och övervakning av elektronisk kommunikation övervaka allt som Snowden eller Bradley Manning gjorde på sina datorer, enligt Europadomstolens praxis? Troligen! Det är väl till stor del detta som Klass handlade om, men idag måste inte spionen smuggla ut eller telegrafera oerhörda mängder arkivmaterial till Sovjetunionen, utan kan snabbt läcka detta till Wikileaks, preventiva åtgärder blir därför i statens ögon nödvändiga på ett annat sätt. Hade en underrättelsetjänst dessutom kunnat starta ett sådant program oavsett något politiskt medgivande? Ja, om man inte förutsätter att Obama ljuger om vad han visste om NSA.

Bland annat till följd av 11:e septemberattackerna verkar staterna på allvar ha riktat in sig på att skapa ett system där man kan slå till innan brottet inträffat. Men även handlingar liknande brott mot rikets säkerhet och spioneri kan som synts nu på sista tiden även användas för att sprida information de flesta anser bör komma upp i ljuset. Genom att bygga upp ett system som i förtid kan stoppa en viss typ av brott, riskerar vi att whistleblowers på höga positioner i samhället blir en omöjlighet, de som sitter tillräckligt högt upp är redan screenade för att ha rätt åsikter.

Vilken lösning föreslår jag på konflikten mellan krypteringstekniken i förhållande till polisens tvångsmedel?

Som de teoretiska kriminalfall jag gått igenom pekar på, får krypteringstekniken en oerhörd påverkan på klassiska tvångsmedel, och ryggmärgsreflexen torde vara att ropa på ett förbud, eller statlig kontroll, över hur tekniken kan användas. Hemlig dataavläsning verkar vara det lösningsförslag som det lagts mest fokus på i det avseendet.

Jag tror dock, när man har min tidigare diskussion om övervakning som bakgrund, och betänker teknikutvecklingen och fenomenet big data, att man ser att frågan inte är riktigt så enkel och att man lätt missar det positiva som krypteringstekniken kan medföra. Om vi vill undvika ett framtida storskaligt kontrollsamhälle, verkar säker krypteringsteknik vara det enda som kan hålla information gömd från staten, mer eller mindre autonoma underrättelsetjänster, och andra starka aktörer som vill utnyttja sig av den moderna teknikens möjligheter. Som forskarna var inne på har vi nu med hjälp av den moderna tekniken möjligheten att bygga upp antingen ett storskaligt övervakningssamhälle, eller ett effektivt skydd för den enskilde. Efter en lång tids katt-och-råtta lek, där staten efter lång tid agerat mot en teknisk företeelse, lagstiftningen blivit omsprungen, staten återigen agerat osv., har vi istället nått fram till en punkt där lagstiftningen riktar in sig mot själva kärnan i förtrolig kommunikation och ett relativt fritt internet.

Folket i bild/Kulturfront till att Leander omedelbart avskedades från sin anställning på Marinmuseet i Karlskrona. Först 1997, efter att Leander fått avslag i samtliga instanser, även i Europadomstolen där Sverige hänvisade till rikets säkerhet , fick han både skadestånd och tillåtelse att se akten där endast informationen om hans val av parkeringsplats fanns nedtecknad. http://www.sydsvenskan.se/kultur--nojen/rent-mjol-i-fel-pase/

Kryptering och den moderna tekniken ställer alltså slutligen övervakningsresonemanget på sin spets, och manar till eftertanke.

Baserat på vad jag kommit fram till om riskerna med övervakning och den snabba tekniska utvecklingen, tror jag att man måste titta efter helt andra lösningar på den här problematiken.

Min slutsats rörande den här frågeställningen baseras på tron att lagstiftaren och vi jurister måste ha ett helhetsperspektiv, och inte bara titta på vad en lag säger, och vilket skydd en domare kan ge. Vi måste även se på hur lagen kan missbrukas, precis som Tysklands generalparagrafer en gång missbrukades.

När ett lagförslag som har en oerhört stor potential för missbruk läggs fram, eller man som i Europadomstolens praxis ser en tendens växa fram mot ett samhälle där möjligheterna till anonymitet utraderas, kan man inte blunda för de olika möjligheter lagstiftningen möjliggör genom att bara titta på syftet i det konkreta fallet, och vilket skydd som finns inbyggt i lagstiftningen.

Detta blir ett ”de små stegens tyranni” och ”vägen till helvetet är kantad av goda avsikter”. Juridiken har genom krypteringstekniken nu istället möjlighet att värna individens rättigheter genom att skydda företeelser som kryptering av data och anonymitetstjänster, möjlighet att skapa ett effektivt system för skydd av tryck och yttrandefrihet, där det inte längre bara är grundlagen utan även tekniken som garanterar att vi inte i framtiden får ett system av censur och förtryck. Istället för att medborgarna måste förlita sig på staten och grundlagen som enda garant för att det fria ordet inte inskränks, kan tekniken skapa möjligheten att staten istället får förlita sig på medborgarna.

Det är enligt mig först på det sättet juridiken kan bygga ett effektivt skydd för personlig integritet, inte genom att, som Europadomstolen hittills gjort, steg för steg kapitulera för statens krav och låta ett gigantiskt övervakningssystem växa fram, färdigt för att missbrukas.

Vad kan då lagstiftaren göra för att komma åt kriminaliteten, om nya tvångsmedel för att komma åt krypteringstekniken inte tillåts?

Jag tror att lagstiftaren måste sluta gå efter lågt hängande frukt, utan våga se vad som orsakar problemen i samhället. Även om varje individ punktbevakas kommer brott att begås.[297] Även om övervakning kan förhindra vissa mord och vissa terrorattentat, kommer andra att lyckas. I takt med att samhället blir allt mer högteknologiskt och även en förödande biologisk attack skulle kunna vara inom en terrorists räckvidd[298], bör man

[297] Jmf. fallet där den s.k. gryningspyromanen kom undan polisens punktbevakning http://www.sydsvenskan.se/sverige/gryningspyromanen-anhallen/
[298] http://www.nytimes.com/2012/03/01/science/maker-says-bird-flu-virus-not-as-dangerous-as-thought.html?_r=0

allvarligt ifrågasätta de nuvarande metoderna. Ju tidigare vi gör detta, innan tekniken hunnits utvecklas alltför mycket, ju bättre! Varje år som går åt till en evig strid mellan lagstiftning och teknik är ett förlorat år i det avseendet.

Den rimligaste lösningen måste istället vara att man tittar på de självklara saker man kan göra som inte förintar den personliga integriteten. Varför sitter barn och chattar med främlingar, och vågar inte berätta för sina föräldrar att de blir utpressade? Bör man ifrågasätta hur samhället är uppbyggt när det bygger på ett allt stressigare och osäkrare yrkesliv med mer övertid, och att småbarn redan vid ung ålder ska lämnas in på dagis? Kan man ge så mycket resurser till skolan att lärare hinner ta sig tid och uppmärksamma tecken hos en elev på att något en dag inte står rätt till?

Varför kan missbrukare, som trots allt är de som finansierar hela narkotikaverksamheten, få gå utan hjälp i årtionden? Varför låter man globala storföretag göra miljardvinster samtidigt som man drar in på den offentliga sektorn medan hela stadsdelar förfaller vilket leder till gängbildning, arbetslöshet, kriminalitet och att grupper ställs mot varandra?

Vad finns det för orsaker till att människor är beredda att utföra självmordsattentat mot länder? Kan man ta bort incitamenten till detta istället för att med allt mer inskränkande metoder försöka stoppa attentaten innan de begås?

Lagstiftaren har valt att bekämpa vår tids stora problem med en repressiv övervakningsapparat, istället för att ta tag i roten till problemet. Först när detta uppmärksammas, och vägen mot mer övervakning stängs för staten, går det att rätta till de verkliga orsakerna. Här har juridiken en oerhört viktig roll att fylla genom att stänga dörren för enkla lösningar, och slå vakt om gamla ideal, på samma sätt som man skyddat exempelvis rätten till en rättvis rättegång i form av oskuldspresumtionen, höga beviskrav och rätten till tystnad. Att då som Olle Abrahamsson verkar vara inne på, lämna över hela integritetsbegreppets omfattning och skyddsvärde till medborgarnas vid olika tillfällen rådande uppfattning om var gränsen för övervakning går, är då en oerhört farlig väg att gå.

I sammanhanget bör det nämnas att en rätt till anonymitet och säker kommunikation inte kommer omöjliggöra brottsbekämpning som sådan. Många människor som begår brott kommer fortfarande att kunna gripas, med hjälp av klassiska metoder. Visserligen har jag i min uppsats visat att det idag finns ytterst stora möjligheter att både hålla sig anonym och kommunicera utan att avlyssnas på nätet. Men när man direkt vill interagera med den fysiska världen, efterger man det skyddet. Fallet med ”The silk road” där en av sidans säljare greps är symptomatiskt för detta troligen allmängiltiga förhållande mellan den fysiska och den virtuella världen: även om tekniken gjorde köpare och säljare anonyma, finns det ingen möjlighet att sända fysiska föremål som droger anonymt på samma sätt, därför kvarstår här myndigheternas möjlighet att upprätthålla lagen. På samma sätt hade man kunnat tänka sig att, om ledaren för sidan inte hade blivit

avslöjad, rättsväsendets uppmärksamhet trots allt hade riktats mot honom den dag han börjat växla in den förmögenhet i bitcoin han skaffat sig.

Samma förhållande mellan den fysiska och den virtuella världen kvarstår vid annan brottslighet. En fildelare som utnyttjar krypteringstekniken kan bryta mot upphovsrätten i princip riskfritt, men han kan inte sälja fysiska piratkopior utan att riskera att straffas, en extremist kan uppmuntra till våld och hat, men de som omsätter det i praktiken kan gripas, osv.

En rimlig balans mellan krypteringstekniken och hemliga tvångsmedel vore troligen därför att man väljer att endast införa den fysiska delen av hemlig dataavläsning, för att kunna få tag i ett lösenord som knappats in. Till skillnad från den virtuella, där staten får möjlighet att storskaligt genombryta anonymiteten på nätet, kan den fysiska delen bara användas mot människor man har tydliga misstankar mot, människor som har agerat i den fysiska världen och som man av den anledningen redan har kommit på spåren.

De faror för demokratin jag berört, storskalig avlyssning, samkörning av information genom big data, osv., gör sig då inte alls påminda i samma grad, genom dataavläsning i den virtuella världen ger man staten den teoretiska möjligheten att avläsa all digital information och kommunikation, med den fysiska formen skyddas fortfarande i princip all möjlighet till säker kommunikation och anonymt delande av information, och försök att storskaligt missbruka tekniken skulle snabbt avslöjas. Som jag tidigare tog upp skulle dock viktiga fall som det med hunden genomföras enklare och med större chans till framgång. Det är följaktligen en lösning på konflikten som jag förordar.

Det bör dock ifrågasättas om brott där hela utredningarna bygger på att det går att lagra och komma åt all information skall vara fortsatt kriminaliserade. Fildelning är ett brott som tydligt visar på hur möjligheterna till anonym kommunikation måste försvinna om lagstiftningen skall ha avsedd effekt. Andra brott som bara består av information, som läckande av hemliga uppgifter, går trots allt att i efterhand utreda genom att se vem som hade tillgång till informationen.

Givetvis kan en förändrad syn på integritet i kombination med att krypteringstekniken blir allt mer allmänt tillgänglig teoretiskt trots allt få en större påverkan på brottbekämpningen. Polisens möjligheter till infiltration och brottsprovokation måste kanske ses över, ett sådant system skulle troligen vara effektivt för att få fast både terrorister och pedofiler, men skulle inte innebära samma fara för demokratin som ett system som förbjuder anonymitet och säker kommunikation. På samma sätt bör kanske tolkningen av EU:s fria rörlighet som hinder mot en effektiv gränstull omvärderas.
Oavsett vilken väg man i framtiden väljer är det enligt mig av demokratisk vikt att frågan om synen på möjlighet till anonymitet lyfts fram i den akademiska diskussionen. Idag verkar tendensen vara att man tar små steg i

taget mot ett samhälle där den enskilde står naken i förhållande till staten, det bör diskuteras öppet att detta är den väg som vi är mer eller mindre determinerade att gå om man inte ska anlägga ett helt nytt synsätt på integritet och anonymitet i förhållande till straffrätten än vad man hittills har gjort.

Hur ser rättsområdet ut idag vad gäller skyldigheten att uppge lösenordet till krypterad information? Vad har hänt på rättsområdet sedan jag skrev min tidigare uppsats "Kryptering, dekryptering och de mänskliga rättigheterna"?

Som sagt står jag fast vid den tolkning jag tidigare gjorde, att systemet strider mot rätten till en rättvis rättegång enligt artikel 6 i Europakonventionen. Mot detta får ställas att flera stater fortfarande använder sig av systemet, och systemet används relativt frekvent i England.

Jag tror dock att också effektivitetsskäl talar emot systemet, som jag delvis berörde i min första uppsats. I den engelska statistiken ser man tydligt att kravet på dekryptering oftast inte efterlevs, något som ju är logiskt med tanke på att de som sysslar med grov brottslighet eller terrorism förmodligen riskerar högre straff om informationen röjs än vad de riskerar för att vägra uppge lösenordet.

Den största bristen är dock att i varje fall Truecrypt som sagt gör det möjligt att skapa en ”dold” krypterad bit av hårddisken, som det inte går att bevisa existerar. Det enda som borde krävas för att få lagstiftningen att falla på kriteriet ändamålsenlig är alltså att den möjligheten lyfts fram vid en prövning i Europadomstolen, givetvis är en sådan möjlighet något som relativt rutinmässigt kommer att användas av dem som begår allvarliga brott, kombinerat med påståenden om att man glömt lösenordet, som jag tidigare nämnde.

Genom uttalandena i SOU 2013 verkar det dock troligt att man inte ser det som rimligt att införa ett sådant här system i Sverige. Man ska dock komma ihåg att det rests krav både från rättsväsendet och från en riksdagsledamot att man skall hitta ett system för att komma runt kryptering.

Riksdagsledamotens motion visar tydligt på att det fortfarande finns en stor oförståelse för hur tekniken fungerar bland riksdagens ledamöter, ett vanligt program på området, Truecrypt, är som sagt open source vilket i teorin borde omöjliggöra en sådan dold huvudnyckel som han talar om, och ett företag som byggde in ”bakvägar” i sina program skulle nog tämligen snart bli utkonkurrerat, troligen skulle ingen kund, särskilt inte företag, föredra ett program med inbyggda säkerhetsluckor som konkurrenter i teorin skulle kunna utnyttja sig av. Då Truecrypt redan finns ute på internet, är det för sent att försöka stoppa den utvecklingen.
Motionen kommer troligtvis att besvaras med just detta, och hänvisa till att det istället kan finnas ett behov av hemlig dataavläsning. Men för att ett teoretiskt key escrow -system skall fungera krävs det givetvis ett förbud mot

att använda andra program som går runt den skyldigheten. Frågan om den framtida lagligheten att kryptera information, i vart fall med vilket program man vill, i Sverige får därför sägas alltjämt vara öppen.

Min slutsats rörande frågan blir dock att det troligen är hemlig dataavläsning som kommer bli den lösning lagstiftaren väljer. Hemlig dataavläsning står inte i uppenbar konflikt med Europadomstolens nuvarande praxis, som systemet med dekrypteringsföreläggande nog får sägas göra, och det skulle som man ser i fallet med hunden kunna vara betydligt effektivare.

En annan fråga är hur systemet med dekrypteringsföreläggande skulle kunna användas mot juridiska personer, kan dessa göra anspråk på rätten till tystnad enligt Europakonventionen? Då samma stora brister i effektivitet gör sig gällande även när tvångsmedlet används mot företag, och det även skulle kunna vara möjligt för enskilda ansvariga på företaget att hävda att de inte kan röja informationen eftersom det skulle gå emot om inte företagets, så i vart fall deras egen, rätt till tystnad, så har jag inte närmre utrett den frågan.

- Hur ser den rättsliga statusen för så kallade anonymiseringstjänster ut i dagsläget, och hur kommer lagstiftningen runt dessa troligen att se ut i framtiden?

Jag anser baserat på det jag kommit fram till i min uppsats, att det inte finns något förbud mot anonymiseringstjänster i dagsläget, och att de dessutom är lagliga i den form som de bedrivs idag. Det verkar heller inte i nuläget finnas några direkta planer på att förbjuda dem.

Å andra sidan pekar mycket på att den enda anledningen till att man underlät att lagstifta mot anonymiseringstjänster från början var att man inte förstod sig på tekniken, och att man inte gjort det senare gissar jag främst beror på att man inte ville skapa en ny intensiv debatt liknande den vid införandet av lagen om signalspaning eller genomförandet av datalagringsdirektivet. Som jag kommit fram till tidigare verkar Europadomstolens praxis medföra att staterna faktiskt förr eller senare måste skapa möjligheter att ta sig runt den här typen av tjänster.

Då jag kommit fram till att det bara skulle behövas en liten förändring i lagen om elektronisk kommunikation för att tjänsterna skulle tvingas lagra data och därmed i praktiken bli verkningslösa, kanske bara ett uttalande från PTS om tolkningen av lagen, får det anses utrett att de är mycket sårbara för exempelvis ett framtida direktiv från EU, som riksdagspartierna är tvingade att införa.

Detta skulle dock skapa nya problem, exempelvis skulle man inte utan ett effektivt kontrollsystem kunna hindra att människor använder anonymiseringstjänster belägna i utlandet. Inget skulle heller hindra att den organiserade brottsligheten skapade egna tjänster som, även om de stängdes ned, snabbt skulle kunna återställas likt ”The silk road”. Decentraliserade system som TOR är rimligen också svårare att komma åt.

Slutligen vore ett förbud mot anonymiseringstjänster inkonsekvent med det stöd som bland annat SIDA lämnat till utvecklingen av anonymitetstjänsten TOR. Att gå från att hävda att anonymitet på internet är något livsviktigt för demokratin, till att skapa system för att komma runt tjänsterna (som rimligtvis kan kopieras av repressiva stater), är ett väldigt långt steg.

Med allt det i beaktande tror jag att det kommer att dröja en tid innan vi ser ett förbud eller åtgärder som gör systemet med anonymitetstjänster ineffektivt. Att sådana åtgärder en dag kommer, om inte Europadomstolen ändrar sin syn på integritet, får däremot anses säkert.

Den väg Europadomstolen valt banar nämligen vägen för ett system med en allvetande stat, där tekniken utnyttjas för att kontrollera själva informationsflödet i samhället, där anonymitet blir omöjlig och endast de som inte har något alls att dölja, vare sig för staten eller för andra människor, verkligen skyddas av Europakonventionen. Tidigare i historien har enskilda kunnat gå samman, och i hemlighet spridit radikala idéer, som slutligen lett till en omvälvning av samhället. Detta är nog en minst lika stor del av vårt historiska arv som många grundläggande juridiska principer. Efter många falska varningar, verkar vi slutligen stå nära den punkt då detta i teorin kan komma att omöjliggöras.

7 Källförteckning

Artiklar

Agrell, Wilhelm, FBI – brottslighetens främsta fiende, Populär Historia, 7/2008,

Palfreyman, Brendan, Lessons from the Brittish and American approaches to compelled decryption, Brooklyn Law Review, vol 75:1 (tillgänglig via databasen HeinOnline)

Abrahamsson, Olle, Integritetsskydd med eller utan förnuft, SvJT 2009 s. 421

Peczenik, Aleksander, Juridikens allmänna läror, SvJT 2005 s. 249

Richards, Neil, The Dangers of Surveillance, tillgänglig via: http://www.harvardlawreview.org/symposium/papers2012/richards.pdf

Tryckta källor

Foster, Steve, Human rights and civil liberties, upplaga 2, Storbrittanien, 2008.

Modéer, Kjell, Juristernas nära förflutna, Tyskland , 2009

Black, Sharon, Telecommunications Law in the Internet Age, Morgan Kaufmann, USA 2002

Danelius, Hans, Mänskliga rättigheter i Europeisk praxis, upplaga 1:3, Stockholm 2000

Rose, Christopher, Office of Surveillance Commissioners Annual Report of the Chief Surveillance Commissioner to the Prime minister and the Scottish ministers for 2012-2013 HC 577 SG/2013/98, England 2013

Klamberg, Mark, FRA:s signalspaning ur ett rättsligt perspektiv, SvJT, 2009

Holmgren, Johan, Kryptering, dekryptering och de mänskliga rättigheterna, Lund 2012

Andersson Sus, Laurin Fredrik, Jankov Petra, Digitalt källskydd –en introduktion, Ödeshög 2012

Nicklasson, Larsa m.fl, Problem vid beslagtagande av egendom, Sundsvall, 2008

Sparner, Otto, m.fl., Anonymitetstjänster, Kalmar 2009

Murphy, Maria, The relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases, Irish Journal of Legal studies, vol. 8(2) 2013

Karnov

Ehrenkrona, Carl-Henrik, Lag 1994:1219, lagkommentar not 51, Karnov

Axberger, Hans-Gunnar, Yttrandefrihetsgrundlagen, lagkommentar, inledande not, Karnov

Rättspraxis

RÅ 1999 ref. 76

Klass m.fl mot Tyskland (application no. 5029/71)

Malone mot England (application no. 8691/79)

Kennedy mot England (application no. 26839/05)

Offentligt tryck

SOU 2005:38

SOU 2006/96

SOU 2013:39

Proposition 1997/98:15

Proposition 2002/03:110

Proposition 2006/07:63

Proposition 2011/12:55

Skriftlig fråga 2007/08:507

Svar på skriftlig fråga 2007/08:507

Näringsutskottets betänkande 2008/09:NU11 Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG

Ds 2011:44, Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet

Dnr: 08-12781, Post och Telestyrelsens remissyttrande 2009-03-18

Dnr: 936-2013, Datainspektionen, remissyttrande 2013-09-19

Dnr: R-2005/1309, Sveriges Advokatsamfund, remissyttrande, 2005-11-28

Dnr: 1391-2005, Datainspektionen, remissyttrande 2005-12-02

Dnr: EBM A-2012/0363, Ekobrottsmyndigheten, remissyttrande 2012-10-24

Internationella Juristkommissionen – Svenska avdelningen, yttrande över DS 2011:44 – Polisens tillgång till signalspaning i försvarsunderättelseverksamhet

Vilka tjänster och nät omfattas av LEK? – En vägledning, Rapportnr: PTS-ER-2009:12

Skriftlig fråga till Europeiska kommissionen, Holm, Jens, E-0897/09, 2009

Svar på Europeiska kommissionens vägnar, Barrot, Jacques, E-0897/09, 2009

Europeiska kommissionen, XV D/5022/97 slutlig WP 6 Rekommendation 3/97, Anonymitet på Internet, 1997

Riksdagens protokoll 2010/11:73 2010-03-16

5001/01/SV/slutlig WP 41, Yttrande 4/2001 om Europarådets utkast till konvention om cyberbrottslighet

Motion 2013/14: Ju277

Report from the commission to the council and the European parliament Evaluation report on the data retention directive (Directive 2006/24/EC) COM/2001/0225 final

Lagtext

SFS 2003:389 Lag (2003:389) om elektronisk kommunikation

SFS 1960:729 Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk

SFS 2008:717 Lag (2008:717) om signalspaning i försvarsunderättelseverksamhet

SFS 1942:740 Rättegångsbalk (1942:740)

SFS 2003:396 Förordning (2003:396) om elektronisk kommunikation

SFS 1998:112 Lag (1998:112) om ansvar för elektroniska anslagstavlor

SFS 1991:1469 Yttrandefrihetsgrundlag (1991:1469)

SFS 1949:105 Tryckfrihetsförordning (1949:105)

EU

Direktiv (2006/24/EG) om lagring av trafikuppgifter

Europeiska konventionen om skydd för de mänskliga rättigheterna

Intervjuer

E-postkonversation med Anne-Marie Eklund-Löwinder den 17 november 2013

Telefonkontakt med Peder Cristvall, Post och Telestyrelsen den 23 december 2013

Telefonkontakt med Björn Sellström, chef för Rikskriminalpolisens grupp mot sexuella övergrepp på barn och barnpornografi den 30 december 2013,

Internetkällor

(samtliga kontrollerade den 8 januari 2014)

http://technet.microsoft.com/en-us/library/cc961626.aspx
http://bahnhof.se/priv/extra/anonym
http://lastbit.com/password-recovery-methods.asp#Guaranteed%20Recovery
http://www.truecrypt.org/
http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf
https://www.iis.se/docs/lar-dig-kryptering.pdf
http://www.truecrypt.org/docs/hidden-volume
https://www.iis.se/bloggare/anne-marie/
https://www.iis.se/vad-vi-gor/
https://integrity.st/privacy/
http://www.juridicum.su.se/iri/docs/Bevisfr%C3%A5gor_vid_upphovsr%C3%A4ttintr%C3%A5ng_genom_fildelning_m.m/
http://dmca.cs.washington.edu/dmca_hotsec08.pdf
https://www.iis.se/lar-dig-mer/guider/digitalt-kallskydd-en-introduktion/skydda-kallan-e-post/
https://itunes.apple.com/se/app/kryptos/id404884924?mt=8
bitcoin.org/en/how-it-works
http://bitcoin.org/bitcoin.pdf

https://www.iis.se/docs/sakrare-mobiltelefon.pdf
http://bahnhof.se/priv/extra/anonym
https://www.torproject.org/about/sponsors.html.en
https://www.torproject.org/docs/faq.html.en#WhatIsTor
http://www.folkpartiet.se/politiker/ledamoter-av-riksdagen/johan-pehrson/debattartiklar/fra-och-signalspaning/
http://www.top500.org/statistics/perfdevel/
https://www.iis.se/blogg/anonym-pa-natet/
http://cybernormer.se/scouter-kopplar-internet-till-manskliga-rattigheter/
http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp
http://www.lu.se/lup/publication/3046392

Nyhetsartiklar

(samtliga kontrollerade den 8 januari 2014)

http://www.sydsvenskan.se/sverige/massavlyssning-avslojades--och-makthavarna-teg/
http://www.gp.se/nyheter/varlden/1.2007113-de-knacker-din-kryptering
http://www.sydsvenskan.se/Pages/ArticlePage.aspx?id=812870&epslanguage=sv
http://www.svd.se/nyheter/utrikes/nsa-slar-tillbaka-obama-visste-inte_8662430.svd
http://arstechnica.com/security/2013/10/new-effort-to-fully-audit-truecrypt-raises-over-16000-in-a-few-short-weeks/
http://www.svd.se/nyheter/inrikes/kapade-datorer-vanligare-i-rattsfall_8586848.svd
http://www.dn.se/nyheter/sverige/man-friad-for-barnporr-i-datorn/
http://www.expressen.se/kvp/doktoranden-med-barnporr-i-datorn-friad/
http://sakerhet.idg.se/2.1070/1.62051
http://www.gp.se/ekonomi/1.2161143-en-omstridd-valuta
http://www.gp.se/ekonomi/1.2201671-det-har-ar-bitcoin
http://www.sydsvenskan.se/opinion/aktuella-fragor/det-vore-fullt-mojligt-for-politiken-att-framja-sadana-tekniker-istallet-for-a/
http://www.di.se/artiklar/2011/7/24/droger-kan-bli-ny-natvalutas-fall/
http://swampland.time.com/2013/10/31/the-deep-web-has-washington-worried/
http://www.theguardian.com/technology/2013/oct/15/silk-road-ross-ulbricht-alleged-mastermind
http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website
http://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/
http://help.disqus.com/customer/portal/articles/1389598-statement2das
http://www.di.se/artiklar/2013/12/12/chef-far-sparken-efter-inlagg-pa-avpixlat/
http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5730621

http://sverigesradio.se/sida/gruppsida.aspx?programid=4282&grupp=16907&artikel=5534626
http://www.bbc.co.uk/news/technology-24842410
http://www.sydsvenskan.se/kultur--nojen/storyn-med-stort-s--ett-besok-hos-the-guardian
http://www.dn.se/nyheter/politik/sa-forblir-du-anonym-pa-internet/
http://www.va.se/helgintervjuer/helgintervjun-robin-teigland1-578149
http://www.svt.se/nyheter/ekonomi/bitcoin-rasar-i-varde-efter-kinesisk-blockad
http://www.sida.se/Svenska/Kontakta-oss/For-medier/Debattartiklar/Arkiv-2011/Debattartiklar-2011/Sa-skyddar-Sida-nataktivisterna/
http://www.dn.se/nyheter/varlden/nathandelsplats-for-narkotika-stangd/
http://www.dn.se/nyheter/sverige/nataktivister-ska-fa-svenskt-bistand/
http://www.dn.se/nyheter/sverige/allt-fler-svenskar-anonyma-pa-natet/
http://sverigesradio.se/sida/artikel.aspx?programid=1646&artikel=5089677
http://edition.cnn.com/2012/03/29/tech/super-computer-exa-flop/
http://www.svd.se/kultur/kulturdebatt/anonymiteten-skapar-trollen_6375562.svd
http://www.dn.se/debatt/lat-oss-bejaka-maktens-overvakning-av-vara-liv/
http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5241785
http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5618974
http://www.sydsvenskan.se/opinion/aktuella-fragor/det-vore-fullt-mojligt-for-politiken-att-framja-sadana-tekniker-istallet-for-a/
http://pcforalla.idg.se/2.1054/1.72937
http://www.sydsvenskan.se/kultur--nojen/storyn-med-stort-s--ett-besok-hos-the-guardian/
http://www.dw.de/several-german-states-admit-to-use-of-controversial-spy-software/a-15449054-1
http://www.realtid.se/ArticlePages/200609/22/20060922082335_Realtid597/20060922082335_Realtid597.dbp.asp
http://www.bbc.co.uk/news/uk-politics-21726612
Jmf. http://www.svd.se/nyheter/inrikes/laila-freivalds-avgar_302444.svd
Jmf. exempelvis http://www.dn.se/nyheter/sverige/greenpeace-inne-pa-karnkraftverk
http://www.svd.se/nyheter/utrikes/bradley-manning-doms-till-35-ars-fangelse_8442090.svd
http://www.sydsvenskan.se/kultur--nojen/rent-mjol-i-fel-pase/
http://www.sydsvenskan.se/sverige/gryningspyromanen-anhallen/
http://www.nytimes.com/2012/03/01/science/maker-says-bird-flu-virus-not-as-dangerous-as-thought.html?_r=0
http://www.svt.se/nyheter/sverige/pedofil-utnyttjade-anonymitetstjanst
http://sakerhet.idg.se/2.1070/1.62051
http://www.dn.se/kultur-noje/sa-hanterar-svenska-tidningar-nathatet/

8 Bilaga 1

Hej!

Jag håller just nu på att skriva mitt examensarbete på juristlinjen, där jag behandlar frågan om krypteringstekniken och hur den påverkar nuvarande tvångsmedel, exempelvis beslag och hemlig telefonavlyssning.

En intressant fråga när det gäller metoder för hemlig övervakning är självklart hur man ska se på dem i förhållande till den personliga integriteten. Min uppfattning är tyvärr att det är en fråga som problematiserats alldeles för lite inom den juridiska doktrinen, både författare, lagstiftare och domare verkar rörande överens om att man kan tillåta i princip vilken form av övervakning som helst, hemlig telefonavlyssning, hemlig rumsavlyssning, övervakning av elektronisk kommunikation, osv., bara den är reglerad i lag och användningen övervakas av en domstol.

I mitt arbete analyserar jag bland annat ett förslag till nytt tvångsmedel, hemlig dataavläsning, som i korthet gör det möjligt för staten att exempelvis via datorvirus komma åt information som krypterats i syfte att hålla denna hemlig, eller avslöja identiteten på människor som gömmer sig bakom så kallade anonymiseringstjänster för att göra sig anonyma på internet. Man motiverar integritetsintrånget även här med att det är proportionerligt med hänsyn till syftet.

Under juristlinjen har vi bland annat läst om teorier om rättvisa och rättigheter, och hur det finns diametralt olika åsikter som båda underbyggs av tunga argument, exempelvis Robert Nozik vs. John Rawls. Jag är därför ute efter tunga namn med en annan syn på integritet än den som staten för fram, gärna författare som anser att varje människa är berättigad till en fredad zon gentemot staten när det kommer till att vara anonym, att kunna kommunicera med andra människor utan att riskera att avlyssnas, eller att kunna ha möjligheten att hålla information hemlig även för staten. Detta för att kunna analysera juridiken och förslagen från en annan synvinkel.

Finns det sådana åsikter i litteraturen, eller är rådande konsensus att det inte finns någon absolut rättighet att hålla information dold för staten? Att den enskildes intresse av att vara anonym alltid måste vika om det behövs för att skydda samhället mot terror, spionerі eller grov brottslighet?

Jag personligen kan se stora problem i att man bygger upp ett omfattande övervakningssystem som även om det i nuläget används för att bekämpa grov brottslighet, med bara ett antal lagändringar istället skulle kunna användas för att i princip cementera ett politisk maktläge genom att beröva människor möjligheten att anonymt kunna kritisera systemet, bilda opinion och konspirera mot makten.

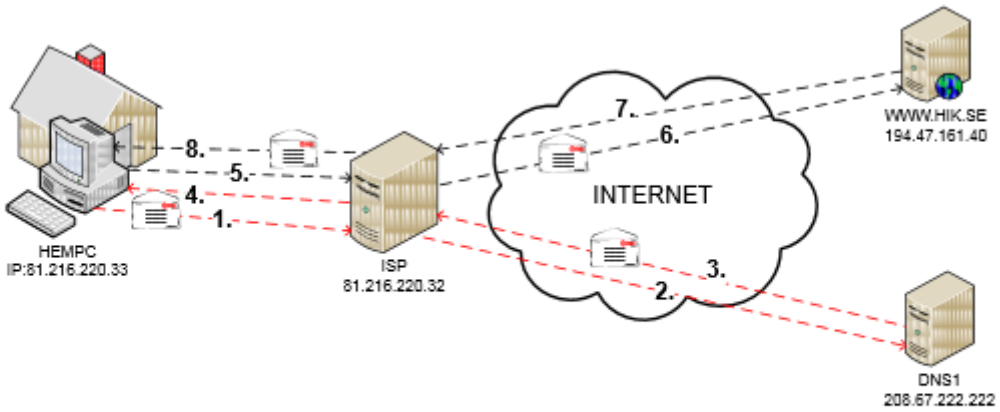
Nog måste det finnas författare som delar de åsikterna?

Med vänliga hälsningar,

Johan Holmgren

9 Bilaga 2

I det första fallet används ingen anonymitetstjänst. Informationen som sänds går att fånga upp och läsa både i användarens dator och på internet. Det är också möjligt att koppla användarens IP-nummer till agerande på nätet, då internetleverantören (ISP) som tidigare nämnts har en skyldighet enligt datalagringsdirektivet att spara sådana uppgifter. Se figur 2 [299].



Figur 2 - IP-paketets väg utan anonymitetstjänst.

I det senare fallet används en anonymitetstjänst. Illustrationen visar hur den information som sänds mellan anonymitetstjänsten och användaren är krypterad, och därmed inte kan avlyssnas. Den krypteras och dekrypteras endast i användarens dator respektive anonymitetstjänstens, och kan alltså avlyssnas först på internet, där anonymitetstjänsten är den enda avsändaren och mottagaren och användarens agerande alltså inte kan knytas specifikt till denne. Skulle mottagarservern i sin tur ha stöd för kryptering, så som sker vid exempelvis bankärenden över internet, kommer informationen inte vara möjlig att avlyssna där heller.

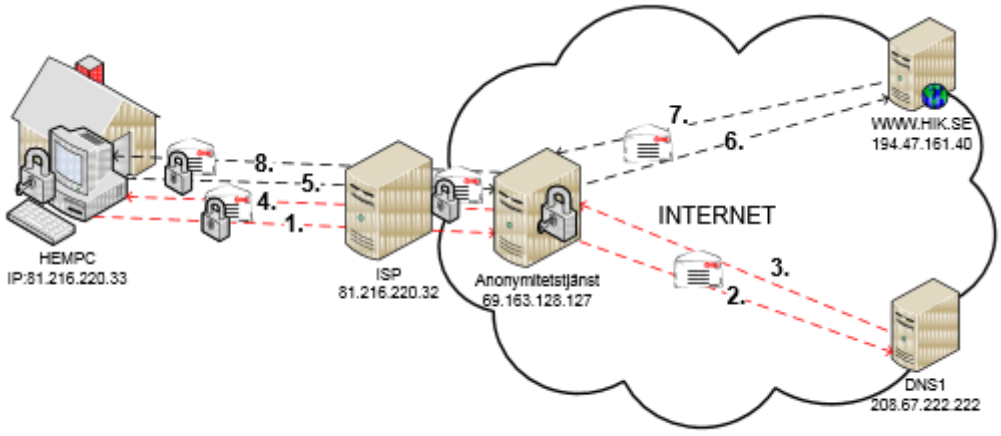


Bild 1 - IP-paketets väg med anonymitetstjänst.

[299] Sparner m. fl, Anonymitetstjänster, 2009, s. 11

Observera att om informationen redan från början var krypterad, exempelvis i form av ett krypterat e-postmeddelande eller telefonsamtal, förblir den krypterad även efter att ha lämnat anonymitetstjänsten! Denna ger endast ett ”extra lager” kryptering. Se bild 1[300].

[300] Sparner m. fl, Anonymitetstjänster, 2009, s.13