GÖTEBORGS UNIVERSITET

Att reglera individers beteende på Internet

En kvalitativ studie om personlig integritet som en viktig aspekt i diskussionen kring övervakning och Internetfiltrering

To regulate the behavior of individuals on the Internet

A qualitative study on privacy as an important aspect in the discussion of surveillance and Internet filtering

LISA BRADLEY
NATHALIE CARLBERG

Kandidatuppsats i Informatik

Rapport nr. 2014:011
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2014

Abstrakt

Det har skett en kraftig ökning av högteknologisk övervakning. Övervakning föreslås nästan alltid som ett färdigt svar på en bred variation av säkerhetsfrågor. Samtidigt har det skett en ökning av kriminella aktiviteter på nätet. Det finns därmed ett stort intresse att använda Internetfiltrering för att reglera individers beteende på Internet. De senaste åren har allt fler stater valt att begränsa innehåll på Internet, där barnpornografi är det innehåll som flest stater idag blockerar tillgången till. Detta har i sin tur gett upphov till nya risker, där initiativet att skydda samhället genom att införa Internetfiltrering samtidigt utgör ett hot mot den personliga integriteten. Denna uppsats syftar att undersöka hur organisationer resonerar kring personlig integritet, övervakning och Internetfiltrering som ett verktyg för att bekämpa spridningen av barnpornografi på Internet. Vi ställde frågan;

Hur förhåller sig organisationer till personlig integritet vid användning av filtreringsteknik för att reglera individers beteende i relation till barnpornografi?

För att besvara frågeställningen utförde vi en kvalitativ studie på fyra olika organisationer som använder sig av olika typer av verktyg för övervakning och Internetfiltrering. Vi valde att använda oss av intervjuer som insamlingsteknik, och gjorde därefter en kvalitativ analys av den insamlade datan. Den huvudsakliga slutsatsen stödjer till stor del forskningen inom ämnet. Det vi kan se utifrån vår studie är att organisationers förhållanden till personlig integritet påverkas av; vilket syfte organisationer använder filtreringsteknik för att reglera individers beteende. Samt vilket beteende det är som övervakas, och till vilken utsträckning. Bransch och företagskulturen påverkar detta förhållande, samt att organisationer separerar på arbetstid och fritid.

Nyckelord: Övervakning, Internetfiltrering, personlig integritet, reglera beteende, barnpornografi.

Abstract

There has been a sharp increase in high-technology surveillance. Surveillance is almost always proposed as a complete response on a wide variety of safety issues. At the same time, there has been an increase in criminal activity online. There is therefore a considerable interest in using Internet filtering to regulate the behavior of individuals on the Internet. In recent years, many countries have chosen to restrict content on the Internet, where child-abusive material is the content that most states currently block access to. This has caused a rise to new risks, where the initiative is to protect society by introducing Internet filtering, while posing a threat to privacy. This essay explores how organizations reflect on privacy, surveillance and Internet filtering as a tool to stop the spread of child-abusive material. We asked the following question;

How do organizations relate to privacy when using filtering technology to regulate the behavior of individuals in relation to child-abusive material?

To answer the research question we conducted a qualitative study at four different organizations that use different types of tools for surveillance and Internet filtering. We chose to make interviews for our data collection. We then made a qualitative analysis of the collected data. The main conclusion supports research on the subject. What we can see from our study is that organizations' relationships to privacy is affected by; the purpose for which organizations use filtering technology to regulate the behavior of individuals, which behavior is being monitored, and to what extent. Industry and corporate culture affect this relationship, and how organizations separates work and freetime.

Keywords: Surveillance, Internet filtering, privacy, regulate behavior, child-abusive material.

TACK

Vi vill tacka NetClean Technologies Sweden AB, speciellt Mattias Shamlo och Anna Borgström för all hjälp på vägen. Vi vill även tacka Björn Sellström för värdefull information i början av vårt arbete. Vi vill också tacka alla intervjupersoner som ställde upp på så kort varsel och tog er tid och bidrog med värdefulla svar till denna uppsats slutresultat.

Slutligen vill vi även tacka vår handledare, Marie Eneman som har lett oss på rätt spår genom hela arbetet. Marie tog sin tid och gav oss viktig feedback, handledning och stöd. Tack!

Innehållsförteckning

1. Introduktion

Informationsteknologi (IT) har medfört betydande fördelar för individer och organisationer. Användningen av IT har möjliggjort att stora mängder av information snabbt och enkelt kan nyttjas av personer. Den har även gjort det möjligt för personer att på ett lättare sätt interagera sinsemellan utan att ta hänsyn för geografiska avstånd (Näringsdepartementet, 2011). IT som har så många positiva effekter kan dock missbrukas och användas för brottslig verksamhet (Wall, 2007). Det finns ett antal växande kriminella aktiviteter på nätet, där den största är upphovsrättsintrång. Ett allvarligt växande exempel som den här uppsatsen tar upp är barnpornografi (Murray, 2013; Davidson & Gottschalk, 2011). Termen barnpornografi är kriminaliserad (Eneman, 2010a) och refererar till material som skildrar barn pornografiskt (Brottsbalken, 16 kap, 10 a §).

Modern teknologi utmanar traditionell lagstiftning, där tekniska lösningar för att reglera individers beteende blir en respons (Akdeniz, 2008). Ett exempel på teknik som används för att bekämpa den typen av brott är övervakning och Internetfiltrering. Övervakning är ett brett ämne därför har vi valt att göra vissa avgränsningar. Den här uppsatsen tar upp övervakning och Internetfiltrering i stark relation till varandra, där Internetfiltrering hänvisar till att blockera en viss typ av material på Internet. För att sedan upptäcka när den typen av materialet påträffas måste i sin tur användares aktiviteter bli övervakade.

Övervakning föreslås nästan alltid som ett färdigt svar på en bred variation av säkerhetsfrågor. Framförallt sedan den 11:e september, har säkerhet och övervakning varit ett återkommande tema i nyheter (Lyon & Wood, 2012). Övervakning och brottsprevention är tätt förknippade med varandra, med tanke på att kunskapen om brott och försöken att hantera dem, skulle vara omöjligt utan övervakning (Barnard-Wills & Wells, 2012). Det har lett till en kraftig ökning av högteknologisk övervakning i västerländska samhällen, vilket har gett upphov till nya risker. Bland annat introduceras övervakning inom områden där inget brottsrelaterat ännu har skett, och sannolikt aldrig kommer att ske (Haggerty & Ericson, 2000).

Användningen av teknik för att reglera oönskat och kriminellt beteende är känt sedan länge (Eneman, 2010a). Internetfiltrering hänvisar till en mängd olika tekniker för att blockera tillgångarna till en viss typ av material (Murray, 2007; Open Net Initiative, 2014a) som kan vara skadligt för individer (Faris & Villeneuve, 2008). Antalet stater som begränsar tillgång till innehåll på Internet har ökat snabbt de senaste åren (Open Net Initiative, 2014a). Det innehåll på Internet som idag filtreras i flest demokratiska stater är barnpornografi (Olsson, 2010). Dock är de lösningar som finns i dagsläget för att förhindra spridningen av barnpornografi inte tillräckligt bra (Eneman, 2010a). Internetfiltrering som ett initiativ till att styra individers aktiviteter på nätet (Ievdokymova, 2013) kan samtidigt utgöra ett hot mot yttrandefriheten och den personliga integriteten (Östergaard, 2004).

Personlig integritet har blivit allt mer komplex i frågan kring övervakning och Internetfiltrering (Dinev, 2014). Samtidigt som IT utgör ett hot mot den personliga integriteten kan den också bidra till att upprätthålla och åstadkomma den. Bara genom att IT framhäver diskussioner kring ämnet, får oss att vilja skydda den (Bylund, 2013). En färsk undersökning visar att nästan hälften av den svenska befolkningen anser att regeringen inte borde reglera Internet mer än vad som görs idag (Davidson, 2013). Samtidigt så oroar sig inte en majoritet (60%) av den svenska befolkningen om regeringen ser vad de gör på Internet. Nästan 50% av Internetanvändare i Sverige oroar sig inte alls för att företag ser vad de gör på Internet (Davidson, 2013).

Ett stort hot mot internetanvändare och den personliga integriteten är att det blir allt mer aktuellt för regeringar att få tag på personlig information i olika syften (Östergaard, 2004). Det finns ett stort intresse av att påverka individers aktiviteter på nätet (Ievdokymova, 2013). Det finns inte en enskild typ av lösning för problemet när den personliga integriteten hindras eller begränsas. Det är en balansgång mellan att skydda samhället, och skydda individers rättigheter (Östergaard, 2004).

1.1. Syfte och frågeställning

Syftet med studien är att undersöka, hur organisationer resonerar kring personlig integritet, övervakning och Internetfiltrering. Där fokus är att studera hur organisationer ser på frågan kring spridning av barnpornografi, och Internetfiltrering som verktyg för att bekämpa den spridningen. Frågeställningen blir därmed:

Hur förhåller sig organisationer till personlig integritet vid användning av filtreringsteknik för att reglera individers beteende i relation till barnpornografi?

1.2. Avgränsning och definition

I vår rapport är *övervakning,* vilket inkluderar *Internetfiltrering,* samt *personlig integritet,* de tre centrala begreppen. I teoriavsnittet (avsnitt 2) kommer vi därmed att beskriva övervakning stort (avsnitt 2.1.) för att sedan lägga mer fokus på Internetfiltrering (2.1.4.), som är den typ av övervakningsverktyg som vi valt att fokusera på. Vi är medvetna om att yttrandefrihet är ett återkommande tema när man pratar om övervakning och Internetfiltrering. Vi har gjort valet att fokusera på den personliga integriteten. Begreppet personlig integritet kommer därför att utforskas (avsnitt 2.2) då det är en relevant aspekt i diskussionen kring övervakning och Internetfiltrering.

2. Teori

Det teoretiska ramverket är uppbyggt av följande begrepp; *Övervakning* vilket inkluderar *Internetfiltrering,* samt *Personlig integritet*. Begreppen är relevanta då de står i fokus för vår undersökning, där vi studerar hur organisationer förhåller sig till dessa begrepp. Avsnittet kommer att behandla övervakning (avsnitt 2.1) där området kommer skildras utifrån olika synsätt. Därefter kommer sedan Internetfiltrering (avsnitt 2.1.4.) att beskrivas. Begreppet personlig integritet (avsnitt 2.2) utforskas därefter som en viktig aspekt i frågan kring övervakning och Internetfiltrering, i ett ständigt utvecklande informationssamhälle. Teoriavsnittet ligger till grund för för att förstå innehållet i diskussionsavsnittet (avsnitt 7).

2.1. Övervakning

Övervakning är inget nytt fenomen utan har alltid spelat en viktig roll i vårt moderna samhälle (Lyon, 2007), där säkerhet och övervakning idag har blivit en del av vår vardag (Lyon & Wood, 2012). Övervakning sker på många platser och i många situationer att det har blivit en integrerad del i vardagen. Övervakning sker exempelvis på bussen, i skolan, på arbetet och andra platser, vilket har gjort det till en vanlig upplevelse (Lyon, 2003; Barnard-Wills & Wells, 2012). I avsnittet kommer vi att lyfta fram synen på övervakning och hur den har förändrats, framförallt sedan den 11e september 2001. Säkerhet och risk kommer även att tas upp som avgörande faktorer. Vidare beskrivs övervakningssystem där Internetfiltrering är den teknik som vi har valt att fokusera på inom området.

2.1.1. Övervakning och säkerhet

Lyon och Wood (2012) menar på att säkerhet handlar om ett mål, ett resultat, medan övervakning kan vara en metod eller ett medel för att uppnå säkerhet. Säkerhet och övervakning har idag blivit allt mer ihopkopplade med varandra. Barnard-Wills (2011) noterar att genom att se övervakning som säkerhet begränsas frågor som ställs till huruvida övervakningen är effektiv eller inte och om övervakningen är tillräcklig i brottsbekämpande syften för att uppnå säkerhet. Frågor kring lämplighet, och risk för berörda personer utesluts. Övervakning används ofta som ett medel för att uppnå säkerhet (Lyon & Wood, 2012), och associeras ofta med något negativt (Lyon, 2007). Skälet till varför övervakning införskaffas kan däremot variera. Exempelvis kan skälet vara att öka produktivitet och effektivitet, eller att skapa konsumenter för särskilda produkter. Det är därmed värt att notera att säkerhet och övervakning ofta blir ihopkopplade med varandra, men att skälet bakom att införa övervakning kan vara av endast strategiska ändamål (Lyon & Wood, 2012).

Övervakning som en metod för att agera proaktivt, innan skada har skett och för att förhindra att den sker, innebär nya risker. Övervakning i straffrättsliga ändamål är generella snarare än specifika. De innefattar brott som redan har begåtts, och ännu ej har begåtts. En risk med initiativet att agera proaktivt är att övervakning introduceras inom områden där inget brottsrelaterat ännu har skett, och sannolikt aldrig kommer att ske. Oskyldiga i det här scenariot uppmuntras att acceptera en viss grad av intrång i deras privatliv i utbyte mot ett skydd som inte bör vara nödvändig (Barnard-Wills & Wells, 2012).

Barnard-Wills (2011) tar upp synen på övervakning, vad som räknas som övervakning, när det är acceptabelt och lämpligt att använda det; i brottsbekämpande syften, kontraterrorism, nationell säkerhet, och som ett tecken på att ett problem uppmärksammas, men även när övervakning ses som oacceptabel och olämplig; som utnyttjar privatlivet och den personliga friheten.

2.1.2. Risk

Sedan den 11e september 2001, har användandet av övervakning ökat radikalt (Lyon, 2003). Säkerhet och övervakning har blivit ett återkommande tema i nyheter (Lyon & Wood, 2012). Där är synen på övervakning främst en polisiär aktivitet (Barnard-Wills, 2011). Säkerhetsindustrin ses nu som en ekonomisk sektor i sig själv (Lyon, 2007), och har vuxit i takt med det ökade intresset för risker, och tekniska lösningar såsom övervakningsteknologi (Fuchs, 2013; Lyon & Wood, 2012). Övervakning föreslås som ett färdigt svar på en rad säkerhetsproblem. Detta sker i tron om att övervakning, och särskilt högteknologisk övervakning är det bästa sättet att bekämpa brott och terrorism (Ericsson 2007).

O'Neil (2005) lägger fram att risk, spelar en avgörande roll i synen på övervakning. Terrorism är ett exempel på en risk där sannolikheten är låg men konsekvenserna upplevs som fasansfulla. Alternativet som gynnas är att eliminera risken istället för att endast hantera den. Stora risker, används som motivering för att bygga ut övervakning i mer vardagliga sammanhang (Barnard-Wills & Wells, 2012). Fuchs (2013) menar på att det moderna samhället idag riskerar att gå emot sina egna liberala värden och värderingar kring yttrandefrihet och mötesfrihet, genom att övervakningstekniker inte endast bekämpar brottslingar och terrorister, utan även utsätter alla för granskning.

Tidigare riktades endast övervakningstekniker mot specifika individer som ansågs vara en risk eller inte förtjänade förtroende ifrån staten. Idag verkar det som att övervakning riktas mot alla, så att den teknik som en gång var reserverad för den misstänkte, nu täcker en större del av befolkningen (Haggerty & Ericson, 2000; Barnard-Wills & Wells, 2012). Garland (2001) argumenterar för hur allt fler länder, särskilt USA och Storbritannien, karakteriseras av en "kultur av kontroll". Vilket innefattar att vi blir allt mindre toleranta och blir allt mindre kapabla att känna tillit. Övervakningsmetoder har varit en viktig aspekt av det moderna samhället, och vuxit fram till att bli en central del av det moderna livet, och därmed växande kulturen av kontroll (Lyon, 2007).

I den virtuella världen där individers identitet är otydlig, har övervakningslösningar ibland svårt att hänga med utvecklingen. Identiteter är centrala i övervakning, men de är också problematiska. Myndigheter använder övervakningstekniker för att fånga gärningsmän, samtidigt som den övervakade populationen försöker stå emot de identiteter som tillskrivs dem. Internet erbjuder stora möjligheter för misstänkta att ändra sin identitet och förvirra övervakningsteam. Övervakningsteknik används i dessa scenarier för brottsbekämpning, men tolkas annorlunda, även av de som antas dra nytta av dess närvaro (Barnard-Wills & Wells, 2012).

2.1.3. Övervakningssystem

Att skydda sig från virus och hackare blir allt vanligt för många företag eller tjänsteleverantör som erbjuder webbtjänster, där övervakningssystem är de vanligaste sätten att göra det på (Östergaard, 2004). Monahan (2010) beskriver övervakningssystem som de som erhåller kontroll över människor genom övervakning och analys av personlig information. Lyon (2007) definierar övervakning som den fokuserade, systematiska och rutinmässiga uppmärksamheten till personlig information. Med fokuserad övervakning, menar han att i slutändan riktar sig övervakning mot individer. Att övervakning är systematisk, innebär att uppmärksamheten på personlig information inte är slumpmässig, utan avsiktlig. Övervakning är också rutinmässig, då det sker som en del av vardagen (Lyon, 2007). Haggerty och Ericson (2000) menar att dagens övervakningssystem innehåller för mycket information om privatpersoner. De skapas olika grupper där privatuppgifterna hamnar, där de anser att anonymiteten försvinner allt mer i takt med övervakningssystem (Haggerty & Ericson, 2000).

2.1.4. Internetfiltrering

OpenNet Initiative (ONI) är ett internationellt samarbetsprojekt (Open Net Initiative, 2014b). De arbetar för att utreda, avslöja och analysera Internetfiltrering och övervakningsmetoder på ett trovärdigt och opartiskt sätt. Målet är att avslöja oavsiktliga konsekvenser av användandet av dessa metoder, och på så sätt bidra till att informera bättre inom detta område. För att uppnå dessa mål utför gruppen avancerade studier, där konsekvenser av nuvarande och framtida trender inom Internetfiltrering och övervakning undersöks (Open Net Initiative, 2014a).

Internetfiltrering hänvisar till en mängd olika tekniker och produkter som används för att blockera tillgångarna till en viss typ av material (Murray, 2007; Open Net Initiative, 2014a), och för att kontrollera användares beteende på Internet (Eneman, 2010b). Dessa tekniska metoder är mycket populära och används ofta av stater eller organisationer för att reglera informationstillgångar (Murray, 2007).

Exempel på tekniska metoder som används vid Internetfiltrering är; teknisk blockering, där tekniker används för att blockera åtkomst till vissa hemsidor, domäner och IP-adresser. Det handlar om att företag som tillhandahåller söktjänster på Internet samarbetar med regeringar för att utesluta olagliga eller oönskade webbplatser från sökresultaten, men även att hemsidor som innehåller olämpligt eller olagligt material stängs ner (Murray, 2013; Open Net Initiative, 2014a). En annan vanlig och effektiv strategi för att begränsa exponeringen till innehåll på Internet är att uppmuntra självcensur. Där man själv reglerar sitt eget beteende på nätet, både i surfvanor och i valet av de innehåll som delas på exempelvis social medier (Open Net Initiative, 2014a).

Internetfiltrering kan ske på fyra olika nivåer;

- *Nationell innehållsfiltrering;* blockeringsteknik som påverkar ett helt lands tillgång till Internet (Open Net Initiative, 2014a).
- *Internetleverantörerna;* den reglering av Internetanvändning som de flesta Internet-användare stöter på görs av deras Internetleverantör. Där de genom att göra designändringar i den digitala miljön har förmågan att reglera viss verksamhet. Den mest uppmärksammade rollen för Internetleverantörer är deras kollektiva roll för att förebygga tillgång till barnpornografi och annat olagligt innehåll (Murray, 2013; Open Net Initiative, 2014a).
- *Institutionell nivå;* där företag, statliga organisationer, skolor och Internetkaféer använder teknisk blockering och/eller självcensur. I vissa länder sker detta på uppdrag av regeringen. Oftare utförs institutionell nivå av Internetfiltrering för att uppfylla de interna målen för institutionen (Open Net Initiative, 2014a).
- *Enskilda datorer;* där mjukvara för filtrering installeras som begränsar en enskild dators åtkomst till vissa webbplatser (Open Net Initiative, 2014a).

Internetfiltrering kan aldrig bli fullständigt effektiv. En orsak är att filtreringsteknik är benägen till antingen underblockering och överblockering. Underblockering hänvisar till filtreringsteknik som misslyckas att blockera åtkomst till allt innehåll som är riktat för censur. Samtidigt så blockerar teknik för filtrering ofta innehåll som de inte har för avsikt att blockera, även känt som överblockering (Open Net Initiative, 2014a). Överflödet av innehåll på Internet innebär att regimer som hoppas att övergripande blockera åtkomst till vissa typer av innehåll måste förlita sig på privata programvaruleverantörer. Detta sätter effektivt kontroll över tillgången på Internet i händerna på privata företag (Open Net Initiative, 2014a).

Fastän de största antalet växande kriminella aktiviteter online består av upphovsrättsintrång, finns det ändå fortfarande ett växande antal av kriminella aktiviteter på nätet som består av produktion, distribution, nedladdning och innehav av barnpornografi (Murray, 2013; Davidson & Gottschalk, 2011). Antalet stater som begränsar tillgång till innehåll på Internet har ökat snabbt de senaste åren (Open Net Initiative, 2014a). Det innehåll på Internet som idag filtreras är mycket varierande. Det kan exempelvis vara politisk eller religiös information, olagligt material eller material som på något sätt kan skada individen (Faris &Villeneuve, 2008; Open Net Initiative, 2014a). Det innehåll på Internet som idag filtreras i flest demokratiska stater är barnpornografi (Olsson, 2010).

Det argument som används mest frekvent för att införskaffa Internetfiltrering är att visst material är skadligt för individer, så därför bör de skyddas från barnpornografi (Eneman, 2010b). Det viktigaste motargumentet för just Internetfiltrering är att det ger en typ av censur vilket utgör ett hot mot yttrandefriheten och integriteten (Olsson, 2010; Murray, 2013). En konsekvens med användning av Internetfiltrering är att individer kan komma att välja att skydda sitt privatliv med hjälp av andra tekniska medel (Ievdokymova, 2013).

2.2. Personlig integritet

I diskussionen kring övervakning, hamnar aldrig frågan kring huruvida den personliga integriteten blir hämmad, långt därifrån. Därför kan man se övervakning och personlig integritet som två sidor av samma mynt. Detta avsnitt kommer att behandla olika perspektiv på vad personlig integritet är utifrån tidigare forskning. Begreppet *personlig integritet* ges ingen kort och koncis definition av i litteraturen, utan det ges olika tolkningar på vad begreppet innebär. I avsnittet kommer vi att behandla begreppet *personlig information*, då det är centralt för personlig integritet. Vidare kommer vi att ta upp personlig integritet i olika miljöer, då synen på personlig integritet varierar utifrån olika situationer.

Bylund (2013) anser att det inte ges en direkt definition av begreppet personlig integritet i litteraturen, utan att det istället ges olika perspektiv (Dinev et. al, 2013). Anledningen till att litteraturen ger olika tolkningar av begreppet är på grund av den osäkerhet som finns kring det. Det som är svårförståeligt måste definieras, dock kan detta göra att man tappar mycket av innebörden av vad begreppet faktiskt betyder (Bylund, 2013; Dinev et. al, 2013). *"privacy seems to be about everything, and therefore it appears to be about nothing"* (Solove 2006 se Dinev et. al, 2013, s. 2) Eftersom begreppet personlig integritet är förenat med så många betydelser, definieras väldigt olika och väcker olika värderingar, tappar begreppet mycket av sin tyngd.

Altman (1975), Bylund (2013) och Westin (1967) har olika syn på vad innebörden av begreppet personlig integritet betyder. För digitala miljöer kan man relatera till det Altmans (1975) argumentation att personlig integritet handlar om jaget, att själv kunna bestämma vad som tillåts, det vill säga att personlig integritet snarare är en definition av vad personer är. Bylund (2013) anser att personlig integritet spelar en viktig roll när det gäller att bevara våra relationer men också när det gäller att bevara vår identitet och självbild. Westins (1967) syn på personlig integritet handlar mer om den personliga informationen och rätten att hantera och kontrollera den. Hans syn på personlig integritet har gjort att nya regleringar och lagstiftningar för datainsamlare har gjorts. Bylund (2013) tar också upp förhållandet mellan personlig integritet och personlig information, där personlig integritet handlar om: "*möjligheten, eller rentav rätten, att kontrollera spridning och användning av personlig information"*(s.7). Det handlar om dataskydd, som är en viktig del för att skydda den personliga integriteten, samt om insamling, hantering och lagring av personlig information (Bylund, 2013).

2.2.1. Personlig information

Ievdokymova (2013) beskriver personlig information som vilken information som helst som identifierar individer. Bylund (2013) tar upp att den personliga informationen sprids idag mer eller mindre helt obehindrat mellan individer, myndigheter och företag. Det har lett till att den personliga integriteten bara uppmärksammas när den hindras eller blir begränsad. Östergaard (2004) tar upp att det finns ett stort hot mot den personliga integriteten, då det blir allt mer aktuellt för regeringar att få tag på personlig information i olika syften. Gränserna på Internets informationsflöde utvidgas, samtidigt som skiljelinjerna mellan den "verkliga" världen och nätet blir allt vagare, vilket leder till att det finns ett större intresse av att påverka individers aktiviteter på nätet (Ievdokymova, 2013).

Samtidigt menar Östergaard (2004) att det inte bara finns en typ av lösning för problemet med när den personliga integriteten hindras eller begränsas, utan att det är en balansgång mellan att skydda samhället, och ett behov av att skydda rättigheterna för individer. Ievdokymova (2013) uppmärksammar även att omständigheterna påverkar huruvida privatpersoner anser att det är acceptabelt att den typen av information är öppen eller inte.

2.2.2. Personlig integritet i den digitala miljön

Dinev (2014) uppmärksammar att frågor som berör information i privatlivet och personlig integritet, har börjat dyka upp allt mer inom IT-området. Detta bottnar i avslöjanden om avlyssningar av nätbaserad trafik som har uppmärksammats allt mer i media. Samtidigt som människor värnar om sitt privatliv, lägger man dock i allt högre utsträckning ut personlig information på nätet och accepterar att bli övervakad. Enligt Dinev (2014) finns det några förklaringar till denna paradox, nämligen 1) människor tror att de bryr sig om sitt privatliv, men gör det inte 2) människor, organisationer och regeringar förstår inte vad personlig integritet är och hur avsaknaden av den kan påverka individen 3) människor vill ha personlig integritet men förstår inte vilken innebörd de mekanismer som styr datainsamlingen har för deras privatliv (Dinev, 2014, s. 97).

Bylund (2013) menar på att man kan se personlig integritet som en process, där processen är till för att ge ett samspel mellan det som är otillgängligt och det som är tillgängligt. Genom att se personlig integritet som en process slipper man att få uppfattningen att personlig integritet är något isolerat eller reserverat. "*om du inte har något att dölja så har du inget att oroa dig för"*(Bylund, 2013, s.26). Uttrycket är något återkommande som inte stämmer när man ser personlig integritet som en process, eftersom det syftar till att skapa en balans för just den situationen, mellan det som är privat och det som inte är det (Bylund, 2013). Altman (1975) argumenterar för att personlig integritet är något vi skapar, inte något vi har. Där han ser det som en dynamisk process där situationer ställer krav på vad som är stängt eller öppet utifrån olika sociala villkor som sker just för stunden. Det sker i samspel med andra inblandade, inte bara utifrån vad enskilda individer prioriterar.

Den fysiska och den digitala miljön har många skillnader, så är den personliga integriteten i stort sätt den samma i båda miljöerna, inställningen till integritet kan däremot ses som olika (Bylund, 2013). En annan likhet mellan de fysiska och digitala miljöerna är att det personer uttrycker eller säger har samma styrka i båda miljöerna. Skillnaden ligger snarare i uttrycket personer gör när de säger det, vilket försvinner nästintill helt i den digitala miljön (Bylund, 2013). Samtidigt kan IT bidra till den personliga integriteten, då IT kan skapa nya möjligheter att bibehålla och åstadkomma den. Bara genom att IT framhäver diskussioner kring ämnet, får oss att vilja skydda den (Bylund, 2013). Samtidigt tar Brin (1998) upp att skadan som kan ske av anonymitet på nätet är mycket större än i något annat medium. Ibland måste man nå identiteter för att kunna upprätthålla vem som bär ansvaret.

3. Svensk lagstiftning gällande barnpornografi

Termen barnpornografi refererar till material som skildrar barn pornografiskt (Brottsbalken, 16 kap, 10 a §). Det finns olika typer av barnpornografiskt material såsom bilder, film, ljudupptagningar och även innehållet varierar från poseringsbilder av barn till material där barn utsätts för sexuella övergrepp (Eneman, 2010a). Barnpornografi är enligt svensk lagstiftning kriminaliserat enligt följande:

10 a § *Den som*
1. skildrar barn i pornografisk bild,
2. sprider, överlåter, upplåter, förevisar eller på annat sätt gör en sådan bild av barn tillgänglig för någon annan,
3. förvärvar eller bjuder ut en sådan bild av barn,
4. förmedlar kontakter mellan köpare och säljare av sådana bilder av barn eller vidtar någon annan liknande åtgärd som syftar till att främja handel med sådana bilder, eller
5. innehar en sådan bild av barn eller betraktar en sådan bild som han eller hon berett sig tillgång till döms för barnpornografibrott till fängelse i högst två år.
(Brottsbalken, 16 kap, 10a§)

Begreppet barnpornografi är missledande, vagt och tar bort allvaret för vad det porträtterar (Gillespie, 2008). Den främsta anledningen är att barnen blir utsatta för att skapa den typen av material (Murray, 2013). Istället borde barnpornografibegreppet heta ”dokumenterade sexuella övergrepp” (Sheldon & Howitt, 2007). Trots den kritiken till begreppet kommer den här studien dock att använda begreppet barnpornografi, då det används i svensk lagstiftning.

Sedan 90-talet har IT-brottssektionen vid Rikskriminalpolisen i Sverige arbetat emot barnpornografi[1]. På senare år har de utvecklat ett samarbete med Internetbranschen för att på ett mer effektivt sätt ta itu med spridningen av barnpornografi, genom att kombinera juridisk och teknisk reglering (Eneman, 2010a). Idag använder många företag, statliga organisationer, skolor och Internetkaféer, Internetfiltrering för förhindra och blockera tillgången till barnpornografi (Open Net Initiative, 2014a). Det som är föremål för filtrering inom ramen för denna studien är Internet innehåll.

1 Björn Sellström Kriminalkommisarie, IT-brottssektionen, Rikskriminalpolisen, intervju den 12 mars 2014.

4. Metod

För att besvara vår frågeställning och uppnå vårt syfte, valde vi att genomföra en kvalitativ studie, kring hur organisationer förhåller sig till personlig integritet och övervakning. Studien är genomförd på fyra olika organisationer som använder sig av olika typer av verktyg för övervakning och Internetfiltrering. Vi valde att använda oss av två olika typer av insamlingstekniker; ostrukturerad intervju och semi-strukturerad intervju. I syfte att besvara frågeställningar kring faktiska förhållanden och faktiska skeenden utförde vi även en litteraturstudie (Patel och Davidsson, 2011). Litteraturstudien låg även till grund för upplägget av de ostrukturerade intervjuerna, samt de semi-strukturerade intervjuerna.

4.1. Fallstudieobjekt

I vår studie valde vi att analysera ett verktyg som heter *ProActive*. ProActive fungerar som ett antivirus-program, där skillnaden är att det söker efter redan identifierad barnpornografi. På stationära och bärbara datorer ute på företagen, (det vill säga på institutionell nivå, på enskilda datorer), där programvaran är installerad, så tittar programmet på alla filhändelser som sker på datorerna. Programmet skannar även trafiken som sker på Internet. När en fil öppnas eller en hemsida besöks, tittar programmet på filen eller adressen till hemsidan, och verifierar om materialet är känt sedan tidigare. Om så är fallet, att materialet är känt sedan tidigare av Rikskriminalpolisen eller andra poliskontakter, så får företaget ett larm. Ingenting lämnar företaget, utan företaget väljer själva att dela med sig av informationen vid ett larm[2].

4.2. Ostrukturerade intervjuer

Vi valde att utföra tre ostrukturerade intervjuer med endast öppna frågor, med större utrymme för svarsalternativ (Krag Jacobsen & Nilsson, 1993). Detta i syfte för att samla in information och utforska en mängd olika ämnen (Rogers et al. 2011; Patel och Davidsson, 2011). De ostrukturerade intervjuerna låg sedan till grund för upplägget till våra semi-strukturerade intervjuer, och kompletterade de material vi redan hade fått ut ifrån litteraturstudien, eftersom det är en fördel att ha goda förkunskaper inom det område som ska studeras med hjälp av en kvalitativ intervju (Patel & Davidsson, 2011).

En ostrukturerad intervju gjordes med Björn Sellström, kriminalkommisarie på Rikskriminalpolisen. Inför intervjun skapades fyra teman (se bilaga 1) som lämnade mycket utrymme till egna resonemang, som exempelvis synpunkter på hur människor tänker kring olika ämnen (Esaiasson et.al, 2003). De två senare ostrukturerade intervjuerna gjordes med anställda på företaget till fallstudieobjektet. Inför intervjun skapades fyra teman (se bilaga 2) på samma sätt som den tidigare ostrukturerade intervjun. Vårt val att genomföra tre ostrukturerade intervjuer var väldigt tidskrävande (Patel & Davidsson, 2011), i synnerhet med tanke på att vi även transkriberade två av dem (Rogers et al. 2011; Patel & Davidsson, 2011). Däremot gav intervjuerna oss användbart underlag, och relevant förberedelse inför de semi-strukturerade intervjuerna. Vi valde att endast transkribera de delar av intervjuerna vi ville använda oss av, för att minska på arbetsbördan (Rogers et al. 2011).

2 Mattias Shamlo, Chief Technology Officer, NetClean Technologies Sweden AB, intervju den 7 april 2014.

4.3. Semi-strukturerade intervjuer

Vi valde att utföra fyra semi-strukturerade intervjuer, med fem olika personer. Som underlag för intervjuerna använde vi oss av en intervjuguide (se bilaga 3). Intervjuguiden var uppdelad i fyra olika teman, där intervjupersonerna fick utrymme att svara på frågorna med egna ord (Patel & Davidsson, 2011). Intervjuguiden var baserad på både stängda och öppna frågor (Rogers et al. 2011). Samtliga intervjupersoner fick tillgång till intervjufrågorna i förväg, då detta var ett önskemål ifrån två av personerna. Vi valde sedan att skicka ut intervjufrågorna till de resterande tre, därmed fick alla samma möjlighet att gå igenom frågorna, och förbereda sig inför mötet. Intervjuerna varade mellan 25-45 minuter. Anledningen till att tidsintervallet på intervjuerna varierade så mycket, berodde på att under en av intervjuerna deltog två intervjupersoner.

Samtliga intervjuer genomfördes på respektive företag där intervjupersonen arbetar, för att underlätta för dem. Vi valde att spela in intervjuerna via mobiltelefon, som ett alternativ istället för att enbart föra anteckningar under intervjun (Rogers et al. 2011). Innan intervjuerna påbörjades informerades intervjupersonerna om syftet med intervjun och att den var konfidentiell (Patel & Davidsson, 2011). Intervjupersonerna fick även skriva under ett inspelningsmedgivande (se bilaga 4). Samtliga semi-strukturerade intervjuer transkriberades och analyserades tätt inpå inspelningstillfället.

4.4. Urval

I vår studie valde vi att intervjua fem olika personer, på fyra olika företag. Företagen var olika stora, och inom olika branscher. För att upprätthålla intervjupersonernas krav att vara konfidentiella i denna uppsats valde vi att inte ta med exakt storlek eller vilken bransch företagen tillhörde. Anledningen var för att undersöka om svaren varierade beroende på bransch eller storlek, huruvida detta var en avgörande faktor. Vi är medvetna om att vi hade fått en mer fyllig bild om vi hade gjort fler intervjuer på fler branscher, eller gjort samtliga intervjuer inom en bransch. Men eftersom inget av de alternativen blev genomförbara för oss, valde vi att utföra en bredare undersökningen, i utforskande syfte.

Vi valde att ta kontakt med två företag som vi visste använder sig av ProActive verktyget. Detta för att kunna jämföra, och ta fram ett tema till intervjuerna som handlade just om det verktyget. Vi valde sedan att ta kontakt med ytterligare två företag själva, som vi inte visste ifall de använde sig av det verktyget. Anledningen till att vi valde att ta kontakt med två företag själva, var för att få ett bredare perspektiv på Internetfiltrering, och undersöka hur de resonerade kring ett liknande verktyg såsom ProActive.

Vår intervjuguide bestod av fyra olika teman (Patel & Davidsson, 2011) (se bilaga 3); *Bakgrundsfrågor, Övervakning, Internetfiltrering* och *Personlig integritet*. Under samtliga intervjuer valde vi att beröra tre av dessa teman, beroende på om företaget använde sig av ProActive verktyget eller inte. Därmed så ställdes frågor kring Bakgrundsfrågor, Internetfiltrering och Personlig integritet till företag som vi visste använde ProActive. Medan de övriga två företagen besvarade frågor kring Bakgrundsfrågor, Övervakning och Personlig integritet istället.

Rogers et al. (2011) argumenterar för att semi-strukturerade intervjuer skall innehålla samma teman under samtliga intervjuer. Samtidigt noterar de att den mest lämpliga tekniken för en intervju beror på syftet med intervjuerna och omständigheterna. Eftersom vårt syfte var att studera hur organisationer förhåller sig till personlig integritet och övervakning, så berör samtliga intervjuer frågor kring just dessa två ämnen. Därutöver berör intervjuerna vårt fallstudieobjekt.

Vi är medvetna om att ett större antal intervjupersoner hade kunnat ge oss ett ännu tydligare underlag till studien, men eftersom vi var tvungna att anpassa oss efter en viss tidsram, så anser vi att fyra intervjuer som underlag är tillräckligt. Genom de personer vi intervjuade fick vi en tillräcklig spridning och bild av läget för att uppnå vårt mål. Nedan presenteras de olika intervjupersonerna och deras roll på företagen:

Intervjuperson 1: *Bolagsjurist.*

Intervjuperson 2: *IT-Säkerhetsansvarig.*

Intervjuperson 3: *Driftansvarig.*

Intervjuperson 4: *Ärendehantering, System och Administration.*

Intervjuperson 5: *IT-Chef.*

Intervjuperson 1 och 2 valdes ut utifrån vår kontakt med företaget till fallstudieobjektet och vilken kontakt intervjupersonen hade med dem. Intervjuperson 3,4 och 5 tog vi själva kontakt med, där intervjuperson 3 och 4 arbetar på samma företag. Gemensamt för samtliga intervjupersoner är att de jobbar med eller är med och tar beslut kring övervakningssystem.

4.5. Bearbetning av insamlad information

För att bearbeta den insamlade informationen, utförde vi en kvalitativ analys av datan. Vi började analysen kort efter att intervjuerna var genomförda, för att fortfarande ha ett "levande" förhållande till materialet (Patel & Davidsson, 2011).

Det första steget i vår bearbetning av materialet var att skapa en överblick, komprimera och hitta samband mellan intervjusvaren (Rogers et al. 2011; Patel & Davidsson, 2011). För att hitta samband så kategoriserade vi den insamlade datan (Rogers et al. 2011) utifrån svaren, med hjälp av en intervjusvarsblankett (Esaiasson et.al, 2003) (se bilaga 5). Intervjusvarsblanketterna skrevs sedan ut på papper, för att ge oss en överblick (Patel & Davidsson, 2011). Vi delade sedan upp blanketterna utifrån intervjufrågorna och valde därefter ut de citat och den struktur, vi ville använda oss av i vårt resultat.

Vår bearbetning av den insamlade datan ledde oss till våra två huvudområden i vårt resultatavsnitt (avsnitt 7); *Övervakning i relation till barnpornografi,* med två underkategorier, *Mer än IT* och *Skillnader mellan branscher.* Samt huvudområdet *Personlig integritet i relation till Internetfiltrering*, också där med två underkategorier *Reglera anställdas beteende* och *Arbete och fritid.* Huvudområdena valdes ut i och med bearbetningen där vi fann ett mönster i intervjuerna mellan övervakning och barnpornografi, samt personlig integritet och Internetfiltrering. Under bearbetningen valdes även de olika underkategorierna ut, eftersom de sågs som viktiga faktorer i diskussionen kring huvudområdena.

5. Resultat

I avsnittet presenteras resultatet från våra semistrukturerade-intervjuer. Avsnittet inleds med att presentera material utifrån *Övervakning i relation till barnpornografi*, med två underrubriker; *Mer än IT* och *Skillnader mellan branscher.* Frågan kring spridning av barnpornografi har lyfts in i diskussionen kring övervakning och filtreringsverktyg. Därefter presenteras material utifrån *Personlig integritet i relation till Internetfiltrering*, även där med två underrubriker; *Reglera anställdas beteende* och *Arbete och fritid*. Där personlig integritet har lyfts in i diskussionen kring Internetfiltrering, och frågan kring barnpornografi. Genom att visa citat från respondenterna ger det en bild av dels hur de formulerade sig och deras uppfattning uppstår då tydligare.

5.1. Övervakning i relation till barnpornografi

En viktig del i diskussionen kring övervakning var att när det handlar om spridning av barnpornografi, sågs det som ett ansvar för företag att agera. Intervjuer med större företag med många anställda såg samhällsproblemet som en viktig fråga att arbete mot. Övervakning och filtreringsverktyg gav företag möjligheten att vara med att förhindra något som är fruktansvärt, oacceptabelt och dessutom olagligt.

Intervjuperson 1 -
Det var den typen av projekt som inte hade så mycket att göra med vår verksamhet, men det har att göra med hur vårt samhälle ser ut, och samhället är vi en väldigt viktig del av, med tanke på att [företaget] är så stort. Vi jobbar väldigt mycket med Corporate Social Responsability-frågor, och vi ser det som viktigt, att inte bara jobba med kärnverksamheten som företag, utan det är andra saker som också spelar roll. Det är inte så att vi installerade eller valde att installera det här verktyget för att vi tror att våra anställda skulle vara mer benägna än andra, att ägna sig åt barnpornografi, eller att använda den typen av material. Utan snarare så ser vi det som ett samhällsproblem och det är ett ansvar för företaget att agera."

Intervjuperson 3 -
"Det är något som ligger varmt åt hjärtat att förhindra att det inte sprids. Det är någonting vi tycker är viktigt och är en del av vårt CSR (Corporate Social Responsibility) arbete, för vi jobbar mycket med CSR och det är en del i att just förhindra spridning. Jag anser att den typen av övervakning är en självklarhet, det hör inte hemma. De anställda är medvetna att vi har den här kollen, och det är ingen som protesterar, utan det är självklart att ha den. dom blir medvetna om att; jag kan inte göra vad som helst på på min dator. Vi har ju en viss typ av övervakning, men det här är lite extra övervakning."

I frågan om Internetfiltreringsverktyg som filtrerar bort barnpornografi, kunde ses som ett övervakningsverktyg, var reaktionerna olika. Samtliga intervjupersoner höll med om att när det gäller ett sådant ämne som barnpornografi så kunde man förbise att det var ett övervakningsverktyg.

Intervjuperson 1 -

"Det är ett övervakningssystem, det är vad det tekniskt är. Sedan är det inte det som är viktigt för oss, i första hand, det här är egentligen ett verktyg, för att i praktiken kunna efterleva vår IT-Policy och våra företagsvärderingar. Det är ett övervakningsverktyg men det kanske inte är så vi tänker på det, men rent tekniskt är de det"

Intervjuperson 2 -

"Vad jag ser det som, är ett larmsystem, som talar om när en övergreppsbild egentligen finns på datorn. Och jag ser inte det som övervakning, på det viset. Ja, den larmar förvisso, men jag skulle nog i det här fallet vilja göra en diffession mellan övervakning och larm."

Intervjuperson 5 -

"Om ni frågar mig så ser jag inte det som övervakning, utan snarare sunt förnuft, att lägga in ett sådant skydd. Man hanterar inte de frågorna om man är en normal människa om man säger så, det är fruktansvärt tycker jag[...] Det ser jag inte som något konstigt över huvudtaget att se över en sådana lösningar. "

Säkerhet togs upp under diskussionerna som en viktig fråga kring övervakning i relation till barnpornografi. Där det handlar om att förebygga kriminella aktiviteter och skydda företaget och de anställda. Intervjuperson 5 beskrev hur deras företag tacklade den frågan:

Intervjuperson 5 -

Vi har väldigt många nät på [företaget] och det är en jättestor fråga för oss just säkerhet, och säkerhet för de anställda, så att man känner sig trygg i sin roll, och att sitta vid sin dator och jobba. Vi jobbar med att förebygga så att man inte skall kunna göra kriminella aktiviteter på [företaget]. vi är ganska hårt styrda här. Det finns en ganska hård gräns för vad man får och inte får göra. Vanlig "normal" surfning får man göra, men all den typen av trafik begränsas. Det är ett ganska avancerat skydd."

5.1.1. Mer än IT

Något som kom fram under diskussionen med intervjupersonerna, var att frågan om att stoppa spridningen av barnpornografi inte var en IT-fråga, eller var inte endast en IT-fråga. Ett beslut att införskaffa ett verktyg för att bekämpa spridningen av barnpornografi, innebar en process där stora delar av organisationen var med och påverkade.

Intervjuperson 1 -
"Det här blir ju ett ganska tvärfunktionellt projekt, man kan inte direkt säga att det bara handlar om juridik, eller bara om personal (HR) eller att det bara handlar om kommunikation. Utan det här tangerar ganska mycket. Det slutgiltiga beslutet var ett gemensamt initiativ av Corporate HR, Corporate Security och Process and IT. Legal var även med på loopen, och Communication. Ytterst skjutsades det upp och informerades till vår koncernledning med vår VD ytterst i spetsen. Det var ett initiativ som inledes med Security men som förankrades ganska brett."

Intervjuperson 3 -
"Det var HR som gick ut med informationen till personalen om att vi hade köpt det här systemet (ProActive) och skulle implementera det. Frågan togs upp på vårt ledningsmöte, med cheferna på de olika områderna. Det är hela verksamheten som har tagit det beslutet, och röstat igenom att det är något vi skall jobba med."

Omständigheterna runt beslutsprocessen var annorlunda enligt Intervjuperson 2 eftersom företaget var styrda av politiska beslut.

Intervjuperson 2 -
" Det är egentligen inte en IT-fråga alls, tycker jag. Utan det är en personalfråga, etikfråga, eller kommunikationsfråga. Hos oss så var det ett politiskt beslut att det skulle finnas ett system som skulle upptäcka barnpornografiskt material på datorn.[...] Och det grundas på att vi ska stå upp för mänskliga rättigheter. Man ska föregå med gott exempel, det är inte svårare en så. [...] Under beslutstagandet så fanns även de anställdas tankar representerade."

5.1.2. Skillnader mellan branscher

I diskussionen kring anställda och deras syn på övervakning och Internetfiltrering, och hur företaget skulle bekämpa spridning av barnpornografi, så varierade engagemanget mellan företagen. Där Intervjuperson 1 berättade om hur implementationsprocessen på deras företag såg ut, där engagemanget var stort. Jämfört med Intervjuperson 2, som såg engagemanget som det motsatta på företaget.

Intervjuperson 1 -

“Engagemanget har varit stort, beslutet var förankrat uppe i koncernledningen. Sedan har vi också jobbat väldigt tydligt under implementationsprocessen att vara transparent, att kommunicera kring detta till så väl anställda som fack och fackföreningar. Fackföreningar är väldigt viktiga på [företaget], vi jobbar väldigt mycket tillsammans med dom. [...] Det är svårt för oss att prata direkt med alla våra anställda.[...] Och de fackliga har ställt sig positiva till detta, det blir ett företag som man är stolt att jobba på. [...] Det har egentligen inte varit några invändningar alls.”

Intervjuperson 2 -

“I och med att det är ett politiskt beslut, så var engagemanget inte jättestort. Och jag skulle snarare som svar säga som såhär, att det var nog väldigt, väldigt starkt motstånd. Vi fick till och med under en period avinstallera NetClean, därför att man på felaktiga grunder visade det sig sen, beskyllde NetClean för att förstöra eller sabotera [specifika]-processer. Man trodde att orsaken var NetClean, men det var det inte. Så därför var det precis tvärt om, engagemanget var det motsatta, man ville inte ha in det här. Sedan är det en kostnad, det är så mycket andra grejer som man vill ha. Och det här ser man egentligen till viss del bara som en kostnad, tyvärr.”

Det fanns olika faktorer påverkade valet att anskaffa ett verktyg för att bekämpa spridningen av barnpornografi. Nedan tas detta upp utifrån tre av intervjupersonernas perspektiv för att visa skillnaden mellan företagen.

Intervjuperson 2 -

“Inte mer än att det var internt motstånd ibland. Att man tyckte att; är det här verkligen nödvändigt? Så att, nej, egentligen inte. Man kan väl säga som såhär; Ja, men det händer väll inte oss, det är väl mer den attityden. Är det verkligen vår uppgift att vara poliser, att hålla koll på andra. Den diskussionen finns också.”

Intervjuperson 4 och Intervjuperson 3 tog upp det faktum, att de inom företaget arbetar i öppna landskap, där kollegor ser vad de gör, och man är måna om att göra rätt saker. Det i sig kan vara en bidragande faktor till att en viss grad filtrering är acceptabel.

Intervjuperson 4 -

“Det många som sitter i öppna landskap om det nu skulle vara en faktor som påverkar, men det tror jag. Sitter man i öppet landskap och ens kollega märker att man sitter och surfar aftonbladet, Facebook och så vidare, klart att dom blir irriterade då. Det är inte så många som sitter i enskilda kontor.”

Intervjuperson 3 -

”Jag tror att mycket av sådana problem löser sig redan ute hos personalen själva, kollegor emellan, i och med våra öppna landskap. Sen tror jag att väldigt många är måna om att göra rätt saker, i vår personal. Jag tror att vi, hela personalen är ganska stolta över vårt varumärke, och vi är inte sådär jättepigga på att smutsa ner det. Det gör ytterligare, att man är rätt okej med viss filtrering. Men det finns ju alltid undantag. Vissa gillar inte att man vet någonting om vad de håller på med.”

En faktor som Intervjuperson 2 tog upp, var att inom deras bransch var man van vid att bli övervakad på ett annat sätt än eventuellt inom andra branscher. Detta i sig gör att ett sådant verktyg inte bidrar till att anställda känner sig mer övervakade.

Intervjuperson 2 -
"I denna [branschen] så är man egentligen ganska van vid, eller hyfsat van vid att bli loggad och att bli granskad. [...]Vi har ju tyvärr en del folk som blir dömda för dataintrång, på grund av att de varit inne [...] där de inte får lov att vara. då tror jag nog att den granskningen inte är störande, men man är nog van vid att det är så här, att man kan bli granskad. Och då tror jag inte att NetClean i sig gör att man känner sig granskad eller övervakad ."

5.2. Personlig integritet i relation till Internetfiltrering

Under intervjuerna diskuterades personlig integritet brett, hur intervjupersonerna såg på begreppet i sig, när de resonerade att den kränktes, och när den stod i samspel med samtliga aktörer. Relationen mellan personlig integritet och Internetfiltrering diskuterades. Exempel dök upp när integriteten inte stod i centrum men även att frågor kring personlig integritet inte skall gå obemärkta. Intervjuperson 3 tog upp att olika typer av människor resonerar olika kring personlig integritet i relation till Internetfiltrering.

Intervjuperson 3 -
"Det finns väldigt många olika typer av människor, vissa tycker säkert att det är bra och andra tycker det är kasst. Jag råkade själv ut för det när jag precis hade börjat på [företaget]. Då var jag ansvarig för mail-system och anti-spam-system. Då råkade jag ut för en användare som blev helt vansining att vi skannade igenom alla mail. Men det var inte så att jag satt och tittade igenom alla mail, utan det var ett automatiserat system som gjorde det. I dagsläget så stoppar vi nog en miljon brev per dag, som är spam, och det är ingen som vill ha dessa breven. Så det är ingen som protesterar mot att vi gör det. Den som hade protesterat hade jag gladeligen vidarebefordrat alla de här mailen till. Jag tror att de flesta är ganska nöjda med att vi faktiskt gör någon form av filtrering på information. Jag tror inte att det är ett jätteproblem, med integriteten."

Intervjuperson 5 tog upp personlig integritet som något som är väldigt viktigt inom IT-världen, och hur det är viktigt att känna trygghet och det är också därför det finns reglerat i lagen. Kommunikation mellan alla skikt inom en organisation ses som en viktig del för att bibehålla den personliga integriteten.

Intervjuperson 5 -
"Personlig integritet om man tittar på IT-världen och det område jag ansvarar för, så handlar det om att känna en trygghet när man jobbar på [företaget]. Man vet sina rättigheter, vad man får och inte får göra. Det är ett samspel mellan oss som arbetsgivare och anställd, som vi har en bra nivå på. Vi har också en bra nivå med facket när det behövs. Att upprätthålla den personliga integriteten är jätteviktig och det finns reglerat i lagen. Vi följer lagar, förordningar samt styrande dokument vi är ålagda att följa."

Intervjuperson 5 -

"Webbfiltrering har de flesta företag, det är sunt förnuft eftersom man signerar trafiken med företagets namn. Så det är klart att man vill få bort det som inte är rätt.[...] Det skall vara säkert för anställda, företag och gäster, det är det vi försöker upprätthålla. I slutändan är det att skapa större tillgänglighet i vårat system. Jag tror på sunt förnuft, och lägga en nivå som fungerar i samråd med anställda, fack och företag."

5.2.1. Reglera anställdas beteende

Att reglera anställdas beteende tolkades olika. Intervjuperson 2 ansåg att man kan reglera anställdas beteende till viss del. Inom företaget var de även styrda av lagar kring vad som måste loggas i deras system. Det tyckte Intervjuperson 2 var något som borde förbättras inom företaget, av säkerhetsskäl.

Intervjuperson 2 -

"Vi reglerar nog inte, vi informerar om att det finns. [...] Å andra sidan om man vet om att det här programmet finns. Då kan man reglera så att man inte gör det på arbetstid, eller på våra maskiner, eller med vår hjälp. Så kanske det ändå är ett steg i rätt riktning att kunna hantera sin livssituation på ett annat sätt."

Intervjuperson 2 -

"Vi har en [lag], som säger att; delar som du gör i våra system ska registreras. Vi har flera system idag som inte gör det [...]. Det kommer att bli ännu mer loggning, och det vet man om. Det pågår även en diskussion om hur mycket vi ska logga och hur mycket vi inte ska logga. Idag så loggar vi var du surfar, på tok för lite, tycker jag. Den centrala loggningen tycker jag är alldeles för kort. Där skulle jag till och med vilja ha, så att man kan spåra en del upp till ett halvår, ett år. Det beror på att vi har en del polisärenden ibland, vi har en del känsliga personalärenden. Där man faktiskt missbrukar maskinerna, datorerna på ett sätt som man inte bör. Och det tar ibland tid att hitta och upptäcka det. Så jag skulle nog vilja ha betydligt mer, och längre loggning än vad vi har idag ut mot Internet."

I frågan kring övervakning och filtrering av barnpornografi, i relation till att reglera personers beteende, hade intervjupersonerna olika synpunkter. Intervjuperson 4 tog upp att ett sådant verktyg inte påverkar den personliga integriteten eftersom den är så nischad. Intervjuperson 2 såg inte heller det som en övervakningsprodukt och därmed kränker den inte integriteten. Intervjuperson 3 ansåg däremot att filtreringsverktyg inkräktar på den personliga integriteten men i frågan kring att stoppa spridningen av barnpornografi anses det acceptabelt.

Intervjuperson 4 -

"Alla tycker att det är en självklar produkt för det tar bara den typen av trafik. Det är inte någon annan trafik som loggas. Så det är ingen som tycker att det är just integritetskränkande, inte någonstans. Det är en självklarhet och det är något som man borde ha."

Intervjuperson 2 -

"I och med att jag inte ser NetClean som en övervakningsprodukt, så känner jag inte heller att den påverkar, integriteten. [...] Nej, jag har inte sätt att det kränker integriteten på det viset."

Intervjuperson 3 -

"Ja, det inkräktar på den personliga integriteten det gör det. Men det är inte ett acceptabelt beteende att hålla på med, överhuvudtaget, och särskilt inte på ett företag. Så jag är ju själv övervakad, det är helt självklart, och det är helt OK. Jag skulle bli jättebesviken på kollegor om jag fick reda på att dom höll på med sådant här. Så absolut, det är en svår fråga, men jag tycker att det är helt okej från min synvinkel. [...] tekniken kan hjälpa oss att leverera mycket bättre tjänster, som jag ser det."

Intervjuperson 1 argumenterade för att en sådan produkt som endast hanterar barnpornografi är väldigt specifik. När det gäller den här typen av verktyg måste man göra en bedömning utifrån om det är ett berättigat ändamål, huruvida det är proportionerligt och att man har kommunikation med de anställda.

Intervjuperson 1 -

"När det gäller NetClean:s produkt är den väldigt specifik, för den inriktar sig på någonting som inte bara är i strid med företagets interna policys, utan någonting som faktiskt är olagligt. Och det är väll det som gör att det kanske "välter över" till att man har en marknad egentligen för en sådan här produkt. Vi känner oss nöjda med att jobba på det sättet, att vi i första hand jobbar genom våra styrdokument, så att man förstår vad som gäller."

Intervjuperson 1 -

"När det gäller den personliga integriteten, så är det väldigt viktigt att man tänker igenom att den här typen av övervakning är för ett berättigat ändamål. Och det har vi gjort bedömningen att, ja, det är det. Är det proportionerligt? det här är ju något som bara fångar upp bilder som faktiskt är klassade som barnpornografi. [...] Det fångar ju inte upp någonting annat.[...]Detta är barnpornografi, inte bara någonting som absolut står i stil med våra egna policys, utan något som är olagligt i de allra flesta länder.[...]Det också jätteviktigt att man är transparent, att man har en kommunikation, att man har haft information till anställda, om varför vi gör de, och vad detta är, och det har faktiskt aldrig varit nån issue. Sålänge man är tydlig med att detta är ett övervakningsverktyg som fångar in just barnpornografiska-bilder som är klassade som barnpornografi av polis."

5.2.2. Arbete och fritid

Skillnaden mellan arbete och fritid var återkommande i samtliga intervjuer där företagets utrustning ska användas till att arbeta på. Eftersom det är företagets utrustning så har även de rätten att bestämma vad som får och inte får göra. Dessutom är det företagets namn som publiceras utåt. Intervjuperson 4, 1 och 5 resonerar kring arbete och fritid nedan:

Intervjuperson 4 -

"Vi har ju en IT-Säkerhetspolicy för våra användare. Där står det hur man skall agera, vad man skall tänka på, även utrustning som, telefoner, datorer och så vidare, är företagets egendom, och vissa saker får man inte göra. På din arbetsplats är det ännu större chans att någon kan logga din trafik. Jag själv har inga problem med att trafik kan loggas och analyseras, för någonstans så sitter man på sin arbetsplats, man sitter och arbetar. Så just den här medvetenheten att det försiggår och att det inte är några större konstigheter, när det händer, det tror jag finns. Men den integritetsfrågan om folk tycker det är bra eller mindre bra, det är nog väldigt spritt"

Intervjuperson 1 -

"Utgångspunkten vi har är att [..] det är [företagets] ägda utrustning. Vi har en IT-policy och vår code-off-conduct, vilket är vårt styrdokument för hur vi anställda skall agera, och hur man jobbar, [...] hur vi använder våra arbetsverktyg. Den här typen av utrustning, det skall man använda för att jobba, det är därför [företaget] köper in det. I och med att det är utrustning som vi äger, så finns det fortfarande sånt användande som vi, även om det är privat, anser inte vara okej, som inte vi vill stå bakom. Eftersom det faktiskt är våra prylar som används för det. Bland annat då, givetvis, pornografi i allmänhet, barnpornografi i synnerhet, är något som är icke okej[...] det är viktigt att hålla isär arbete och fritid. För vi har jättekänslig information som vi lagrar på dessa datorerna."

Intervjuperson 5 -

"Sitter du på [företagets] datorer, så är det faktiskt vårt namn som publiceras utåt när man är inne på olika sidor. Det är klart att vi vill att det skall vara ren trafik som publiceras, när man är här skall man jobba, på luncher och raster är man fri till att nyttja sina datorer efter den nivån som vi har satt."

6. Diskussion

Syftet med studien var att undersöka hur organisationer resonerar kring övervakning, Internetfiltrering och personlig integritet. Där fokus var att studera hur organisationer ser på frågan kring spridning av barnpornografi, och Internetfiltrering som verktyg för att bekämpa den spridningen. Samt hur organisationer resonerar kring den regleringen av personers beteende, och hur detta påverkar den personliga integriteten. I diskussionen kring övervakning i relation till barnpornografi anser intervjupersonerna i linje med Barnard-Wills (2011), att spridningen av barnpornografi är ett kvalificerat syfte att styrka införandet av övervakningsteknik. Flera av intervjupersonerna såg det som ett ansvar för företaget att agera mot det samhällsproblemet. Liksom Barnard-Wills (2011) att ett problem uppmärksammas i och med införandet av ett sådant verktyg.

I frågan om ett verktyg som söker ut och filtrerar bort barnpornografi, kunde ses som ett övervakningsverktyg eller inte, var svaren väldigt olika. I och med att ett sådant filtreringsverktyg sågs som ett tillägg till övrigt skydd, och inte hade något med kärnverksamheten att göra, sågs det inte som ett övervakningsverktyg. Vi menar på att huruvida aktiviteter loggas eller inte är en avgörande faktor om det ses som övervakning, eller inte. Även att det som söks ut är barnpornografi, anser vi blir en ytterligare väsentlig faktor. Om olagligt material aldrig påträffas ses ett sådant verktyg mer som en övervakningskamera som filmar, men inte spelar in.

Säkerhet diskuterades som en viktig fråga kring övervakning i relation till barnpornografi. Lyon och Wood (2012) skriver att säkerhet är ett mål, där övervakning är en metod för att uppnå det målet. Det var något som var återkommande i intervjuerna, att övervakning i brottsbekämpande ändamål, är en viktig del av säkerheten, för att skydda företaget i sin helhet. En annan liknelse var hur hårt styrd de var på några av företagen där de kan se en tydlig parallell med (Lyon & Wood, 2012) att säkerhet och övervakning idag har blivit en del av vardagen.

Under intervjuerna framgick det att intervjupersonerna ansåg att valet med att implementera filtreringsverktyg i brottsbekämpande ändamål, hade ytterst lite eller knappt något med IT att göra utan det var snarare en säkerhetsfråga, ett politiskt beslut, eller en fråga som landade i hela organisationen och inte bara något som IT bestämde. I den frågan kan man dra liknelse med Ericsson (2007) som anser att övervakning föreslås som ett färdigt svar på en bred variation av säkerhetsproblem. Filtreringsverktyg som används för brottsbekämpning, i överensstämmelse vad Barnard-Wills och Wells (2012) antyder, så tolkas dess närvaro olika, även av de som antas dra nytta av verktyget. Vår studie visar att anställda inom olika branscher, tolkar närvaron av övervakningsverktyg annorlunda. Där de anställda var vana vid att bli övervakade, loggade, sågs filtreringsverktyg för hantering av barnpornografi, främst som ett ställningstagande och en kostnad, och ifrågasattes huruvida det var lämpligt och vilken risk det medförde.

I diskussionen kring personlig integritet visar studien i överensstämmelse med Altman (1975) att personlig integritet handlar om jaget, att man själv bestämmer vad som tillåts. Davidsson (2013) visar statistik på att privatpersoner inte oroar sig mycket alls, ifall det blir övervakade på Internet. Samtidigt så antyder Dinev (2014) att organisationer och regeringar inte förstår vad personlig integritet är och hur påverkad individen kan bli ifall den personliga integriteten saknas.

Vår studie gav oss ett oväntat resultat, som visar att personlig integritet är en väldigt viktig del av företagens kultur, trots att statistiken visar på att personer inte bryr sig att företag vet vad de gör på Internet. En parallell som Dinev et.al, (2013) antyder är att begreppet personlig integritet tappar mycket av sin tyngd, då de är förenat med så många betydelser och väcker olika värderingar. Vår studie överensstämmer med Dinev et al. (2013), där vissa företag var väldigt tydliga med att gå ut med information om allt som hände, eller förändrats på företaget så de anställda inte skulle känna sig förda bakom ljuset. Samtidigt som andra företag var mindre tydliga, eller inte gick ut med information på samma sätt, eftersom de ansåg att den personliga integriteten inte var en faktor i diskussionen. Vi menar att det beror på grund av olika antaganden om vad begreppet innebär.

Studien visar på att den personliga integriteten är i stort sätt den samma i både den fysiska och digitala miljön, i linje med vad Bylund (2013) antyder. Där den personliga integriteten anses som väldigt viktig att upprätthålla. Ett sätt att upprätthålla den personliga integriteten är att skapa ett samspel mellan alla inblandade parter i ett företag, genom att skapa en nivå som är accepterad av alla.

I frågan om att reglera anställdas beteende var reaktionen olika beroende på vilket företag vi frågade. Det handlade mycket om ifall företagen var hårt styrda av lagar och regler eller inte. När vi sedan gick in på frågor kring att reglera personers beteende med verktyg som hanterar barnpornografi, ansåg några av intervjupersonerna att det inte påverkade den personliga integriteten alls, då verktyget är så nischat mot en sak. Baserat på våra resultat menar vi att verktyg som hanterar barnpornografi specifikt, inte ses som reglering av ett beteende. I synnerhet inte om det finns verktyg som reglerar mycket annat Internetrelaterat beteende vid sidan om.

Ett ytterligare oväntat resultat av vår studie var att en majoritet inte såg verktyget som en övervakningsprodukt och kunde därför inte påverka integriteten. Samtidigt ansåg en av intervjupersonerna att verktyget kränkte den personliga integriteten. Men eftersom målet att stoppa spridningen av barnpornografi är ett godtyckligt ändamål att stå bakom, så kunde man förbise integritetsfrågan. Det sågs som något som var i linje med företagens egna synsätt.

Vi menar i linje med det som Bylund (2013) diskuterar, att IT inte nödvändigtvis behöver vara begränsande för den personliga integriteten utan att den snarare kan bidra, då den kan stödja etablerade sätt att bibehålla den. IT skapar nya möjligheter till att åstadkomma den personliga integriteten. Bara genom att IT framhäver diskussioner kring ämnet, får oss att vilja skydda den. Studien visar även i linje med vad Östergaard (2004) skriver, att det är en balansgång mellan att skydda samhället, och ett behov av att skydda rättigheterna för individer.

Bylund (2013) tar upp att det är lätt till att den personliga integriteten bara uppmärksammas när den hindras. Vår studie visar på att uppmärksamheten till den personliga integriteten skiljer sig mellan företag, men huruvida integriteten hindrades eller inte, var inte den avgörande faktorn till graden av uppmärksamhet. Där vissa företag i samband med införandet av ett verktyg som motverkar spridningen av barnpornografi, tog upp frågan väldigt aktivt, och andra tog upp det i mindre utsträckning, trots att de ansåg att integriteten kränks av ett sådant verktyg.

Studien visar även i linje med vad Ievdokymova (2013) skriver, att omständigheterna är avgörande i frågan kring inställningen till integritet. Att arbete och fritid var åtskilda omständigheter, var ett återkommande argument i intervjuerna. Intervjupersonerna ansåg att det den enskilda individen gör med företagets resurser är sitt jobb och inget annat. Idag kan man se att linjen emellan jobb och fritid blir allt vagare (Lyon, 2007). Detta var något som intervjupersonerna ansåg att man som anställd inte skulle tänka. När man är på jobbet och surfar så är det företagets namn man representerar, sedan vad man gör på fritiden, det får man bestämma själv.

7. Slutsatser

Frågan vi ställde inledningsvis var: *Hur förhåller sig organisationer till personlig integritet vid användning av filtreringsteknik för att reglera individers beteende i relation till barnpornografi?* Det vi kan se utifrån vår studie är att mycket av litteraturen stämmer överens med hur företag ser på den personliga integriteten, i relation till övervakning och Internetfiltrering. Samtidigt som studien motsäger vissa teorier kring begreppet.

Det huvudsakliga resultatet av vår studie, hur organisationer förhåller sig till personlig integritet är styrt av fyra olika faktorer:

- Där den första faktorn är; *i vilket syfte använder sig organisationer teknik för att reglera individers beteende.* Det kvalificerade syftet till faktorn var att stoppa spridningen av barnpornografi, det är ett ansvar för företaget att göra något åt ett samhällsproblem, som är i linje med företagens egna synsätt. Det ansågs vara ett godtyckligt ändamål, där man till viss del kan förbise integritetsfrågor. Bara genom att införa Internetfiltrering, uppmärksammas ett sådant samhällsproblem. Det som är kritiskt är balansgången mellan att skydda rättigheterna för individer och samtidigt skydda samhället.

- Den andra faktorn är; *vilket beteende det är som övervakas, och i vilken utsträckning*. När det gäller filtreringsverktyg som specifikt hanterar barnpornografi, så sågs inte det som reglering utan snarare som en säkerhet. Eftersom det finns filtreringsverktyg och övervakning som reglerar mycket annat, som påverkar individer mer. Det handlar även om hur mycket aktiviteter som loggas, i relation till om man kan kalla det för övervakning eller ej.

- Den tredje faktorn är; *vilken bransch och hur företagskulturen ser ut.* Vilken bransch som företaget tillhörde, gjorde att de hade olika syn på personlig integritet. Där anställda var mer eller mindre vana att bli reglerade på sin arbetsplats varierade från företag till företag. Även att företagen var mer eller mindre styrda av lagar och regler var också olika. Hur företagskulturen såg ut, hur mycket information som gick ut till de anställda, och hur mycket det anställda brydde sig om vad företaget övervakade varierade. Vilket i sin tur påverkade hur företagen såg på huruvida den personliga integriteten blir kränkt eller inte.

- Den fjärde faktorn är; *att separera på arbetstid och fritid.* Omständigheterna var en avgörande faktor kring inställningen till personlig integritet. Ett återkommande argument var att man skall se en stor skillnad mellan arbete och fritid. Där den främsta anledning var, att det är företagets resurser de använder. Och företagets namn som man signerar trafiken med. Så när du är på jobbet skall du göra ditt arbete, sedan vad de anställda gör på fritiden är deras ensak.

7.1. Studiens överförbarhet och relevans

Studien genomfördes med ProActive som vårt fallstudieobjekt, där syftet var att undersöka hur organisationer resonerar kring personlig integritet, övervakning och Internetfiltrering. Som tidigare nämns har vårt fokus legat i att studera hur organisationer ser på frågan kring spridning av barnpornografi, och Internetfiltrering som verktyg för att bekämpa den typen av spridning. Samtidigt se hur organisationer resonerar kring reglering av personers beteende, och personlig integritet. Därmed anser vi att vår studie och vårt resultat blir överförbart till andra tekniker för att stoppa spridningen av barnpornografi än just Internetfiltrering. Relevansen för vår studie är som vi nämner i vårt teoriavsnitt (avsnitt 2) att övervakning och Internetfiltrering utgör ett hot för den personliga integriteten. Man kan se en upptrappning på stater och organisationer som införskaffar övervakning och Internetfiltrering. Samtidigt visar vår studie på att den personliga integriteten är en viktig och relevant aspekt i diskussioner kring övervakning och Internetfiltrering ute hos organisationer.

7.2. Förslag till vidare forskning

I vår studie har vi studerat hur organisationer förhåller sig till användning av filtreringsverktyg för att reglera anställdas beteende i relation till barnpornografi samt personlig integritet. Vi har enbart lagt vårt fokus på att se vad företag anser om den frågan. Vidare forskning skulle därför kunna vara att gå in mer på individer och se utifrån deras perspektiv. En annan intressant aspekt hade kunnat vara att gå in och analysera företag som valt att inte införskaffa ett sådant verktyg och se hur de resonerar kring det beslutet.

8. Referenslista

Akdeniz, Y. (2008). *Internet Child Pornography and the law.* Ashgate, Surrey, England.

Altman, I (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Monterey, CA: Brooks/Cole Pub. Co. Inc, Libraries, Australia.

Barnard-Wills, D. Wells, H. (2012). Surveillance, technology and the everyday. *Criminology & Criminal Justice,* 12(3), ss. 227–237.

Barnard-Wills, D (2011). UK news media discourses of surveillance. *Sociological Quarterly*, 52(4), ss. 548–567.

Brin, D. (1998). *The Transparent Society.* Addison-Wesley, Massachusetts

Brottsbalken, 16 kap, 10 a §, (SFS, 1962:700). *Brott mot allmän ordning*. Stockholm: Justitiedepartementet.

Bylund, M. (2013). *personlig integritet på nätet*. FORES, Stockholm, Sverige.

Davidson, J. Gottschalk, P. (2011). *Internet child-abusive current research and policy.* Routledge, New York, NY.

Davidson, P. (2013). *Svenskarnas inställning till övervakning via Internet.* http://www.Internetstatistik.se/artiklar/svenskarnas-installning-till-overvakning-via-Internet/ [2014-03-06]

Dinev, T. (2014). Why would we care about privacy. *European Journal of Information Systems,* 23(2), ss. 97–102.

Dinev, T. Xu, H. Smith, H. J. Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), ss. 295–316.

Eneman, M (2010a). *DEVELOPING CHILD PROTECTION STRATEGIES: A Critical Study of Offenders' Use of Information Technology for the Sexual Exploitation of Children.* Diss., Göteborgs universitet. Geson Hylte Tryck, Göteborg, Sverige.

Eneman, M. (2010b). ISPs filtering of child abusive material: A critical reflection of its effectiveness. *Journal of Sexual Aggression, Special Issue on Child Sexual Abuse & the Internet*, 16(2), ss. 223-235.

Esaiasson, P. Gilljam, M. Oscarsson, H. Wängnerud, L. (2003). *Metodpraktikan: Konsten att studera samhälle, individ och marknad* (2:a uppl.), Norsteds Juridik AB, Stockholm, Sverige.

Faris, R. Villeneuve, N. (2008). Measuring global Internet filtering. I Deibert, R. Palfrey, J. Rohozinski, R. Zittrain, J. (Eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press, ss. 5-27.

Fuchs, C. (2013). Societal and ideological Impacts of Deep Packet Inspection Internet. *Surveillance, Information, Communication & Society*, 16(8): ss. 1328-1359.

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society.* Chicago: University of Chicago Press.

Gillespie, A. A. (2008). *Child Exploitation and Communication Technologies*. Russell House Publishing, England.

Haggerty, K. Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology,* 51(4): ss. 605–622.

Hamilton, S. (2004). *To what extent can libraries ensure free, equal and unhampered access to Internet-accessible information resources from a global perspective?* Diss., Royal School of Library and Information Science, Denmark. Copenhagen.

Ievdokymova, I (2013). ACTA and the Enforcement of Copyright in Cyberspace: the Impact on Privacy. *European Law Journal,* 19(6): ss. 759–778.

Krag Jacobsen, J. Nilsson, B (1993). *Intervju: konsten att lyssna och fråga*. Studentlitteratur, Lund, Sverige.

Lyon, D. (2003). *Surveillance after September 11*. Polity Press, Cambridge, England

Lyon, D. (2007). *Surveillance Studies: An Overview.*Polity Press, Cambridge, England

Lyon, D. Wood, M. (2012). Security, Surveillance, and Sociological Analysis. *Canadian Sociological Association*, 49(4): ss. 317-327.

Monahan, T. (2010). *Surveillance in the Time of Insecurity.* New Brunswick, NJ: Rutgers University Press.

Murray, A. D. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. Routledge-Cavendish, Abingdon, Oxfordshire, England.

Murray, A. D. (2013). *Information Technology Law: The law and society* (2:a uppl.), Oxford University Press, Oxford, United Kingdom.

NetClean (2014). *Integrerar avancerad teknik med socialt ansvar - för ett tryggare samhälle.* https://www.netclean.com/sv/om-oss/ [2014-03-06]

Näringsdepartementet (2011). *It i människans tjänst - en digital agenda för Sverige.* (Rapport 2011:12) Stockholm: Näringsdepartementet.

Olsson, R. A. (2010) *Sökes: En Teknisk lösning på ondskans problem. En Guide om filtrering av innehåll på nätet.* Stiftelsen för Internetinfrastruktur, Stockholm, Sverige.

O'Neil, P (2005). Complexity and counter-terrorism: Thinking about biometrics. *Studies in Conflict and Terrorism*, 28(6): ss. 547–566.

Open Net Initiative (2014a). *About Filtering*. https://opennet.net/about-filtering [2014-05-07]

Open Net Initiative (2014b). *About Open Net Initiative*. https://opennet.net/about-oni [2014-05-07]

Patel, R. Davidson, B. (2011). *Forskningsmetodikens grunder – Att planera, genomföra och rapportera en undersökning*, Studentlitteratur, Lund, Sverige.

Rogers, Y. Sharp, H. Preece, J. (2011). *Interaction Design - Beyond Human-Computer Interaction* (3:e uppl.), John Wiley & Sons, Ltd, Chichester, West Sussex, England.

Sheldon, K.. Howitt, D. (2007). *Sex Offenders and the Internet.* John Wiley & Sons, Ltd, Chichester, West Sussex, England.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, Cambridge, England.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum, New York, USA.

Östergaard, S.D. (2004). European Trends in Privacy: How can we increase Internet security and protect individual privacy? *Journal of Systemics, Cypernetics and Informatics*, 2(2): ss. 25-29.

Bilaga 1 - Intervjuguide 1

1. Polisens arbete (övergripande):

- Hur bekämpar polisen barnpornografi i dagsläget?

2. Internetfiltreingsverktyg

- Vad använder sig polisen för produkter/tjänster idag?

- Fördelen/Nackdelen med teknologin? Risker? Önskemål som teknik som hjälpa till med?

3. Övervakning

- Känner du att det finns någon bransch idag som du tror skulle varit bra om den var mer (mindre) övervakad?

- Ifall du befann dig på ett företag som hade detta system, hade du känt dig övervakad då?

- Hur ser du på frågan kring att privatpersoner (oskyldiga i detta scenariot) känner sig övervakade i vardagen?

- Nödvändig, övervakning?

4. Framtiden

- Finns det något typ av system/hjälpmedel som du känner saknas i dagsläget?

Bilaga 2 - Intervjuguide 2

1. Företaget

- ProActive

2. Framtiden/utveckling

- Utvecklas ProActive-verktyget specifikt för vissa kunder? (på samma sätt som polisen?)
Är det olika från kund(företag) till kund(företag)?

- Är det någon produkt/funktion som ni saknar eller som utvecklas just nu?

3. Kunder

- Nuvarande kunder

- Potentiella kunder

- Företag som nekat tjänsten?

4. Övervakning/Personlig integritet

- Känner du att det finns någon bransch idag som du tror skulle varit bra om den var mer (mindre) övervakad?

- Ifall du befann dig på ett företag som hade detta system, hade du känt dig övervakad då?

- Hur ser du på frågan kring att privatpersoner (oskyldiga i detta scenariot) känner sig övervakade i vardagen?

- Nödvändig, övervakning?

- Diskussion kring två citat från litteraturen:
“Jag har inget att dölja, så jag bryr mig inte om jag är övervakad”
“Om du inte vill att någon ska se vad du gör på Internet, kanske du inte borde göra det”

Bilaga 3 - Intervjuguide 3

Namn:	
Datum för intervju:	
Plats:	
Genomförd av:	
Andra noteringar:	

Bakgrundsfrågor
- Be informanten att presentera sig själv kort och vilka arbetsuppgifter denne har inom bolaget.
- Hur många anställda har [företaget]?

Övervakning
- Hur ser [företaget] på övervakning av sina anställdas aktiviteter på Internet?
- Använder [företaget] någon typ av produkt för att reglera anställdas aktivitet på Internet. Exempelvis webbfiltrering?
- Har ni hört talas om företaget?
- Har det varit uppe i diskussion att anskaffa ett liknande verktyg?
- Hur ser ni på den typen av övervakning av de anställda?

Internetfiltrering
- Hur såg processen ut på [företaget] från att ni blev kontaktade, fram till att ett beslut togs om att [företaget] skulle använda sig av ProActive verktyget?
- Vilka faktorer/anledningar under processen låg till grund för att [företaget] sedan valde att anskaffa ProActive verktyget?
- Fanns det faktorer/anledningar under processen som gjorde att [företaget] inte skulle anskaffa ProActive verktyget?
- Vilka var med och beslutade om att anskaffa ProActive verktyget?

Personlig Integritet
- Ser ni ProActive verktyget som ett övervakningsverktyg?
- Hur tänker ni angående den här typen av teknik i relation till den personliga integriteten?
- Hur ser ni på att reglera anställdas beteende med hjälp av ProActive verktyget?
- Bör de anställda vara mer reglerade i deras användande av företags resurser, och i deras Internetanvändning?
- Ser ni några utmaningar och/eller oönskade konsekvenser med användning av denna typ av teknik?
- Övriga tankar - Har du några övriga tankar och funderingar om det vi pratat om idag?

Bilaga 4 - Inspelningsmedgivande

Tack för att du deltar i vår undersökning.

Vi kommer att spela in denna intervju för att kunna gå tillbaka och analysera och citera delar av intervjun som är relevanta för vår studie.

I uppsatsen kommer intervjun att vara anonym.

Läs vänligen nedanstående text och skriv under om du samtycker.

Jag förstår att detta mötet kommer att spelas in.

Jag tillåter Lisa Bradley och Nathalie Carlberg att använda inspelningen som underlag i sitt uppsatsarbete på Göteborgs universitet, vårterminen 2014. Jag förstår att citat och åsikter kan komma att användas i undersökningen och sedan göras tillgänglig i en nationell uppsatsdatabas.

Signatur: _____

Namnförtydligande: _____

Datum: _____

Bilaga 5 - Intervjusvarsblankett

Blankett för att sammanfatta intervjusvar: (Esaiasson et.al, 2003, s.297)

Namn: **Intervjufråga:**
Svaret i korthet:
Belysande citat och exempel:
Egna kommentarer: