LUNDS UNIVERSITET
Rättssociologiska institutionen

LUNDS
UNIVERSITET

Risker i det digitaliserade samhället

Unga vuxnas kunskap och medvetenhet om risker på nätet

Kandidatuppsats: RÄSK02
Vårterminen: 2017

Charlotte Hedenborg & Paulina Kranc

Handledare: Reza Banakar
Examinator: Anna Sonander

Abstract

The purpose of this study is to investigate young adults knowledge and awareness of online crime, and also to examine their attitudes towards the legislation in the area. We also find it interesting to investigate if young adults are worried to become victims of online crime, and if this affects their internet usage. This, because there are risks of entering personal data online. What makes people extra vulnerable to this type of crime is that online risks are more complex and may be more difficult to predict than risks in the physical world. The theory chosen in this essay is Ulrich Beck's risk society in which he brings up different types of risks that can affect its citizens. This theory will be applied to online crime and occurring risks in our high-technological society. Finally, the results in this study have shown that young adult awareness is high, but that the knowledge was relatively low regarding how to protect themselves from online crime and risks. The knowledge was also relatively low on how to protect themselves from becoming victims of online crime. Also, the knowledge of current legislation regarding online crime was also relatively low. Unfortunately, the risks on the internet are greater than some may believe, especially when criminals can be anonymous and data breaches occur without major signs on the victim's computer. The law and social norms should therefore work together to internalize a generally accepted behavior online.

Keywords**:** knowledge, law, online crime, risk and young adults

Innehållsförteckning

1. Inledning

"There is a general problem, that people don't seem to understand that your private data is private for a reason, once it's on the internet, you can't ever drag it back. Its out there forevermore, and thats it. It means you lost it, and someone else can steal it in the future" (Graham Cluley, Facebook follies, 2011).

Citatet ovan av Graham Cluley kan anses spegla många individers beteende på internet. Att dela privata uppgifter online på diverse sociala nätverkssajter är något som blivit allt mer normaliserat. Människor i dagens högteknologiska värld verkar inte ha förståelse för att all den information som publiceras lagras och sparas i cyberspace. Många individer är idag inte medvetna om att data i form av bild eller text som publicerats online alltid kommer att existera i cyberspace, även om denna data raderats av användaren. Ytterligare en intressant aspekt som lyfts fram av Cluley är att om en individ inte är beredd att gå ut på en offentlig plats och ropa ut sina personliga uppgifter, så skall hen inte heller uppge det online på diverse nätverkssajter. Detta är något som framförallt lyfts fram i dokumentären "Facebook förstörde mitt liv" med originaltiteln "Facebook follies" från år 2011 som finns tillgänglig på TV4Play.

I takt med internets utveckling påverkas individers vardag allt mer av att alltid vara tillgängliga och ständigt uppkopplade. Internet kan anses spela en viktig roll i människors liv då tekniken bland annat används för att effektivisera vardagliga uppgifter. Människor använder internet för en mängd samhällsfunktioner som handel av varor och tjänster, sociala nätverk för kommunikation, nyhetsförmedling och informationssök (Larsson, 2014 s. 80). Det går dock att argumentera för både positiva samt negativa aspekter av den högteknologiska utvecklingen som skett. Det har lett till att en mängd forskning genomförts gällande sociala medier och dess verkningar. En del forskning hävdar att sociala medier har bidragit med diverse fördelar för människor, som ökat socialt kapital, socialt och emotionellt stöd eller känsla av välbefinnande. Dock visar annan forskning på att sociala medier även lett till negativa konsekvenser när människor använder sig av sociala medier. De negativa verkningarna kan vara minskad självkänsla, psykisk ohälsa, känsla av isolering, svartsjuka, konflikter eller nätmobbning (Jung Kim & Hancock, 2015 s. 214). Jung Kim och Hancock lyfter även fram att människor tenderar att se sin egen framtid som mer positiv än andras, och att negativa händelser inte kommer hända en själv. Exempelvis har människor en tendens att tro att det finns en större chans för att andra att utsättas för olycka, och att individen själv klarar sig undan negativa händelser. Denna optimistiska bias hos människor gällande potentiella risker och fördelar med att använda sig av

Facebook och andra sociala nätverkssajter kan därmed förklaras med att människor ofta underskattar deras sårbarhet att utsättas för negativa händelser. Detta kan därmed öka människors risktagande samt oförsiktighet när de använder sig av internet (2015, s. 214–215).

De negativa aspekter som internetanvändande medfört har kommit att uppmärksammas allt mer inom kriminologin och andra vetenskapliga områden. Framför allt då internet tillfört nya redskap för människan att kunna utföra brott på nätet. Dessa typ av brott behöver nödvändigtvis inte vara nya, dock har de tagit en ny form då de kan utföras online, både anonymt samt på global nivå. Detta skapar i sin tur problematik gällande lagstiftning som har svårt att hänga med i den tekniska utvecklingen, vilket i sin tur underlättar brott på nätet (Wall, 2013 s. 437, 447).

Utifrån ovan nämnda är det av intresse att i studien undersöka vilken kunskap och medvetenhet unga vuxna har om de risker som finns på nätet. Vi finner det även intressant att få en inblick i ungas internetanvändande, hur de eventuellt skyddar sig mot nätbrott och vilken attityd de har för svensk lagstiftning gällande denna typ av brott. Det blir därmed relevant att undersöka hur den nuvarande svenska lagstiftningen ser ut gällande brott på nätet med fokus på identitet, integritet och personuppgifter. Enligt nationalencyklopedin förklaras begreppet identitet som en individs självbild och att kunna bevisa att en person är den hen utger sig att vara (NE, u.å). Personlig integritet innebär en individs rätt att ha kontroll över vem som skall få tillgång till ens privata information (SFS 1998:204). Personuppgifter går under all slags information som indirekt eller direkt kan kopplas till en fysisk person som är i livet (ibid.).

Frida Andersson, utredare vid Brottsförebyggande rådet, hävdar att kunskapen om nätbrott inom rättsväsendet är relativt låg. Hon menar även att brottsutredningsprocessen blir lidande på grund av den bristande kunskapen om utredningsåtgärder. Det behövs en djupare kunskap och förståelse för nätbrott, samt mer resurser för att kunna utreda dessa brott på ett effektivt sätt som leder till fler uppklarade mål. Det valda ämnesområdet blir därmed intressant och aktuellt då nätbrott är något som uppmärksammats den senaste tiden (Andersson, 2015). Därav finner vi det av stor relevans att lyfta fram detta problemområde i studien. Detta då framväxten av nätbrott samt okunskapen om denna typ av brott har skapat svårigheter och utmaningar för såväl rätten som samhället. Det är även av rättssociologisk relevans då gällande lagstiftning kan anses vara svår att applicera till de nya formerna av brott som sker online. Även Enarsson argumenterar för att lagstiftningen eventuellt ej hänger med i den högteknologiska utvecklingen där traditionella brott har tagit en ny form på nätet (2015). Det kan därmed anses problematiskt då lagen bland annat har i uppgift att skydda samhällsmedborgarna samt ge en

ökad trygghetskänsla i samhället. Kan lagen ej påverka samhället och skydda dess medborgare mot nätbrott, kan rättsväsendet riskera att förlora förtroendet samt tillit (ibid.). Detta högaktuella problemområde gällande brott på nätet kommer därmed att belysas i denna studie och genomföras med hjälp av en kvantitativ enkätundersökning bland unga vuxna. Teorin som kommer tillämpas i den här studien är Ulrich Becks teori om risksamhället.

1.1 Syfte och frågeställningar

Syftet med denna studie är att undersöka kunskapen och medvetenheten kring brott på nätet, men även att undersöka unga vuxnas attityd kring lagstiftningen inom detta område. Vi finner det även intressant att undersöka ifall det existerar en oroskänsla för att utsättas för nätbrott, och om detta påverkar unga vuxnas internetanvändande. Även de risker som finns i samband med internetanvändande kommer att studeras för att få en inblick i om detta påverkar deras handlande online. Detta då det finns risker med att ange personuppgifter, handla varor och tjänster online samt att använda sig av sociala medier. Det som gör människor extra sårbara att utsättas för denna typ av brott är att risker online är mer komplexa och kan möjligtvis vara svårare att förutspå jämfört med risker i det fysiska rummet (Larsson, 2014 s. 81–82). Det skulle kunna innebära att människor möjligtvis ser risker online som mindre allvarliga, vilket eventuellt kan påverka deras risktagande och handlande på nätet. Eftersom nätbrott är ett relativt nytt fenomen är det av stor betydelse att människor får djupare förståelse samt kunskap om risker i samband med internetanvändande. Detta för att samhället ska bli bättre på att skydda sig mot denna typ av brott, men även för att främja det brottsförebyggande arbetet (Andersson, 2015). Utifrån ett rättssociologiskt perspektiv finner vi det även intressant att undersöka unga vuxnas attityd till rättens möjligheter att reglera människors beteende i cyberspace. En egen tanke som växt fram under arbetets gång är huruvida sociala normer eventuellt kan samverka med rätten för att öka människors medvetenhet samt minimera risker att utsättas för nätbrott. Detta då det kan antas vara svårt för lagen att som enda verktyg reglera människors beteende online. Denna tanke har framförallt växt fram under granskning av tidigare forskning gällande reglering av internet samt människors beteende online. Detta kommer även att redogöras för ytterligare under punkt 2.3 som berör reglering av internet.

Frågeställningar som kommer beröras i denna studie lyder enligt följande:

- *Vilken kunskap och medvetenhet har unga vuxna om de risker som finns på nätet gällande integritet och personuppgifter och hur påverkar det deras internetanvändande?*

- *Vilken attityd har unga vuxna till lagstiftningens och rättsväsendets möjligheter att påverka nätbrott?*

- *Hur kan rätten och sociala normer samverka på ett effektivt sätt för att minska risken för nätbrott och öka medvetenheten kring risker på nätet?*

1.2 Avgränsning

För att kunna undersöka medvetenhet samt kunskap gällande nätbrott måste det göras en avgränsning för att arbetet inte skall bli allt för stort och omfattande. Den ekonomiska begränsningen samt tidsbrist har även varit avgörande faktorer i avgränsningen. Vi har därmed valt att rikta in oss på unga vuxna då de är den åldersgrupp som i högst utsträckning använder sig av internet (Oksanena & Keipi, 2013 s. 306–307). Eftersom väldigt många använder sig av internet i Sverige är det extra intressant att undersöka informationskunnigheten, medvetenheten samt risktagande bland unga vuxna gällande deras onlineaktiviteter (Svensson & Dahlstrand, 2014 s. 8).

För att nå ut till ett större antal respondenter har vi valt att framställa och genomföra en enkätstudie, både online samt i pappersform. Webbenkäterna publicerades på våra privata facebookprofiler, medan enkäterna i pappersform delades ut på campusområden vid Lunds universitet. Detta för att på så sätt nå ut till vår önskade urvalsgrupp på ett så effektivt sätt som möjligt. Vi tillämpade kvantitativ metod då vi eftersökte statistiska och kvantifierbara resultat. Detta, för att på så sätt få en överblick rent procentuellt hur medvetna unga vuxna är om de risker som finns online, samt vilken kunskap de besitter gällande lagstiftning. En annan fördel med att använda sig av kvantitativ metod är att en stor mängd data kan samlas in och analyseras på relativt kort tid. Med hjälp av kvantitativ metod kan även studiens resultat presenteras i form av diagram, vilket kan ge en ökad förståelse och bättre bild av insamlat material (Denscombe, 2009 s. 364). Eftersom vi haft en tidsbegränsning kan även kvantitativ metod anses som en effektiv metod för denna studie.

I vår avgränsning gällande material insamlat av andra forskare har vi valt att granska ett antal akademiska artiklar samt relevant litteratur inom det valda ämnesområdet. Gällande tidigare forskning har vi haft som mål att helst applicera artiklar som är högst 10 år gamla. Detta då internet ständigt utvecklas och förändras, vilket kräver att informationen är aktuell och riktig.

Det förekommer dock ett antal artiklar som är något äldre då det bidrog med viktig och relevant information för studien.

1.3 Disposition

I den här uppsatsen presenteras totalt sex kapitel med ett antal underrubriker. Det första kapitlet består av en introduktion, syfte, frågeställning samt en avgränsning. I det andra kapitlet berörs tidigare forskning, risker med användande av nätverkssajten Facebook, nätbrott utifrån ett rättssociologiskt perspektiv, reglering av internet samt kortfattat om vad lagen säger. Det tredje kapitlet består av det teoretiska ramverket där Becks teori om risksamhälle kopplas till risker som uppstår i dagens högteknologiska samhälle. Här lyfts även kritik fram mot Becks teori för att visa på objektivitet i val av teori. I det fjärde kapitlet presenteras den valda metoden samt genomförandet av datainsamlingen i form av webbenkäter och enkäter i pappersform. I det här kapitlet redogörs det även för valet av frågor till deltagarna, undersökningsdeltagare samt för- och nackdelarna med den valda metoden. I det femte kapitlet redogörs det för analys och diskussion av studiens resultat och slutligen avslutas uppsatsen med ett sjätte kapitel där slutsatser och avslutande kommentarer presenteras.

2. Tidigare forskning

Under det senaste decenniet har en kategori av brottslighet på nätet uppstått och som undersöks särskilt inom kriminologin. Nätbrott är en relativt ny typ av brottsliga handlingar som omfattar alla de sätt där datorer och andra typer av bärbara elektroniska enheter som mobiltelefoner och handdatorer kan koppla upp sig till internet och användas för att bryta lagar och orsaka skada. Nätbrott har uppstått och utvecklats med hjälp av internets framgång och de framsteg som gjorts inom informationsteknik. Datorn eller enheten kan fungera som en hjälpreda för att utföra brott men den kan även vara målet för brottet. Brottet kan alltså utföras på en dator och exempelvis ge skador i form dataintrång men det kan även påverka andra icke-virtuella platser (Putnik & Bošković, 2015 s. 569–570). Denna utveckling av internet har medfört risker för att utsättas för en ny typ av brottslighet. Något som framför allt är problematiskt med nätbrott är att det ständigt förändras och förnyas i takt med teknikens utveckling. Nätbrottslingar tar ständigt fram nya verktyg, sätt och metoder för att uppnå sina mål. De samlar in uppgifter och information om ett potentiellt offer från dennes profiler på sociala nätverkssajter. Data som samlas in används sedan för att begå brottsliga handlingar på internet som får konsekvenser i det fysiska rummet (Putnik & Bošković, 2015 s. 570–571).

Det finns även kriminella nätverk som använder cyberspace för att begå kriminella handlingar. Dessa handlingar begås ofta mot godtrogna internetanvändare som använder internet för att bedriva dagliga aktiviteter som att skicka e-post, köpa in varor eller chatta på sociala nätverkssajter. Den snabba internetutvecklingen har skapat utmaningar och begränsningar för lagstiftarens förmåga att reglera lagarna på ett effektivt sätt (Cassim, 2015 s. 69). Domstolarnas arbete försvåras då lagstiftningen har svårt att hänga med i utvecklingen av brott som sker på nätet. Det är inte enbart brott gällande personuppgifter och identitetsstölder som sker online. Något som även förekommer är nya typer av utpressning, nätmobbning och förtal, vilket försvårar polisens och domstolarnas arbete då flertalet av brotten har tagit en ny form (Wall, 2013 s. 437). Wall nämner även att polisens främsta arbetsuppgifter är att hålla kriminella verksamheter borta från gatorna, främja ett säkert samhälle, upprätthålla ordning och genomdriva lagar. Detta blir dock problematisk när olika brottstyper ändrar form och istället begås på nätet (2013, s. 447). Exempelvis kan gärningsmän genomföra brottsliga handlingar helt anonymt vilket försvårar brottsutredningsprocessen. Ett av de stora problemen i att utreda nätbrott är den försvårade identitetsspårningen som orsakas av den anonymitet som finns bland internetanvändare (Nirkhi, Dharaskar & Thakre, 2012 s. 300). Anonymiteten på internet har lett till en större möjlighet för kriminella att begå nätbrott som till exempel identitetsstöld. Detta inträffar när en persons personliga uppgifter som identitetshandlingar erhålls av en obehörig och därefter användas för att begå brott i form av stöld eller bedrägeri (Cassim, 2015 s. 69). Nätbrott avser även brott som exempelvis kreditkortsbedrägerier online samt spridning av barnpornografi eller annat olagligt material (Oksanena & Keipi, 2013 s. 299).

Det kan därmed bli svårt att tillämpa lagstiftning som inte hänger med teknikens utveckling och som inte går att applicera till brott som tagit en ny form (Wall, 2013 s. 453). Det har även bidragit till en växande diskussion om hur olika missbruk och brott på nätet bör styras (Oksanena & Keipi, 2013 s. 299). Cassim lyfter även fram att brott som identitetsstöld belyser behovet av lämpliga lagar som innebär bättre säkerhet inom företag och organisationer som lagrar och hanterar personliga uppgifter. Det är av yttersta vikt att företag och organisationer skyddar individers personliga uppgifter samt annat känsligt material på ett säkert sätt. I sin artikel lyfter Cassim dessutom fram behovet av att utbilda människor om deras rättigheter genom att göra dem medvetna samt vaksamma för risken att utsättas för identitetsstöld (2015, s. 71–72).

Den virtuella världen har en mycket viktig roll i livet för unga människor då de på olika sätt använder sig av internet, särskilt i länder som är ledande inom teknisk innovation (Oksanena & Keipi, 2013 s. 298). Det är framför allt unga vuxna som är sårbara för brott på

nätet och nättrakasserier. Det kan exempelvis röra sig om sexuella trakasserier via chattforum eller annan kränkande behandling via direktmeddelanden eller på bloggar (Saridakis, et al. 2016 s. 320). Onlinetrakasserier omfattar även nätmobbning och forskning tyder på att frekvensen av internetanvändning är relaterad till hur stort antal som viktimiseras. Det vill säga ju frekventare användning av internet, desto större risk löper personen att utsättas för kränkningar online (Saridakis, et al. 2016 s. 321). Vikten av internetanvändarnas medvetenhet gällande risker som finns på sociala nätverkssajter är av stor betydelse för att förhindra viktimisering. Det är även något som sociala nätverkssajter bör informera om då många av deras användare anger allt för detaljerade personuppgifter som kan missbrukas av andra användare (Saridakis, et al. 2016 s. 320).

I en studie utförd av Oksanena och Keipi undersöktes nätbrott i Finland bland olika åldersgrupper där deltagarna var i åldrarna 15–74. Syftet var att se om risken för att utsättas för nätbrott är större bland unga personer än äldre (2013, s. 298). Resultaten visade att unga människor är mer benägna att bli offer för nätbrott än andra åldersgrupper. Förutom att unga är mer aktiva online är unga ofta mindre erfarna om de risker som internetanvändande innebär (Oksanena & Keipi, 2013 s. 306–307). Orsaken till att unga vuxna kan vara mer utsatta för nätbrott kan bero på att de är den åldersgrupp som är mest aktiv i sociala medier och olika chattforum. Detta kan delvis förklara den högre sannolikheten för att bli offer för nätbrott. Framförallt då unga kan vara mer naiva för de risker som kan uppstå på nätet, vilket kan bero på en bristande kunskap. Det framgår även att det finns en skillnad mellan de olika könen, unga kvinnor blir nämligen oftare offer för sexuell värvning och trakasserier jämfört med män (Oksanena & Keipi, 2013 s. 299). Den åldersgrupp som visade sig var mest utsatt för näbrott i Oksanena och Keipis studie var unga i åldern 15–24 (5,3 procent), (se tabell 1, 2013, s. 302). Förutom åldern verkar det även finnas andra faktorer som kan var avgörande för hur stor risk en person löper för att utsättas för nätbrott, bland annat socio-ekonomiska skillnader. Det studien visade på var att unga och högutbildade användargrupper är mer aktiva och villiga att prova nya onlinetjänster och produkter. Vilket i sin tur kan resultera i att de löper större risk för att utsättas för nätbrott (Oksanena & Keipi, 2013 s. 307).

Putnik och Bošković hävdar att unga vuxna är den mest naiva åldersgruppen som använder sig av sociala nätverk, och att de i störst utsträckning lägger upp information och multimediainnehåll på sina profiler som kan missbrukas av andra internetanvändare. Putnik och Bošković nämner även att de vanligaste brotten som drabbar unga vuxna på nätet är framför allt kränkning av den personliga integriteten och missbruk av deras personuppgifter (2015, s. 569). Webbsidor där individer kan lägga upp information om sig själv, som Facebook och

Twitter, är för närvarande mycket populära sociala nätverkssajter bland unga vuxna. Det är även väldigt lättillgängligt då individer kan få tillgång till de här nätverken via datorer men även smartphones. Detta möjliggör ett snabbt och enkelt sätt att kommunicera med andra människor via sociala nätverk online. Det utgör även ett stort risktagande att lägga ut allt för personlig information online ifall någon obehörig skulle få tillgång till detta (Putnik & Bošković, 2015 s. 571). Information som publiceras på sociala nätverkssajter kan missbrukas av andra internetanvändare, exempelvis nätbrottslingar. Många unga vuxna är även ovetande om att det kan utsättas för brottslighet när de ständigt uppdaterar sina profiler på sociala nätverk. Exempelvis uppdaterar människor när de är utomlands, på jobbet eller skriver om annan känslig information. Detta är något som sker på webbsidan Twitter. Där publicerar användarna inlägg om aktiviteter som sker i vardagslivet. Exempelvis vad individerna gör på fritiden, vart de befinner sig och vem de är med. Denna information kan därmed missbrukas för att planera och genomföra brottslig verksamhet som rån, kidnappning, fysiska och psykiska övergrepp vilket kan kränka en individs personliga integritet (ibid.). Internetbaserade sociala nätverkssajter levererar en stor mängd information till gärningspersonen om offret, vilket ger dem ett övertag och en stor möjlighet att utföra en brottslig handling (Putnik & Bošković, 2015 s. 572). För att främja ett säkert användande av sociala nätverkssajter krävs det att unga vuxna får mer information om riskerna kring nätbrott, och att de inte skall dela med sig av allt för personlig information online (Putnik & Bošković, 2015 s. 580).

Numera har e-post blivit ett sätt för människor att kommunicera med varandra över internet. Det har dock även skapat möjligheter för personer att med hjälp av e-post begå nätbrott. Exempelvis går det att spamma en annan persons e-post för att på så sätt kapa dennes identitetsuppgifter. Detta för att kunna komma åt känsligt material eller information i form av bilder, bankuppgifter eller liknande (Nirkhi, Dharaskar & Thakre, 2012 s. 300). Identitetsstöld är självklart inte något nytt fenomen. Det är dock ett brott som tagit en ny form med bakgrund av internets framväxt. Förr i tiden var så kallat "container dykning" det vanligaste sättet att få tag på dokument innehållande personuppgifter. Gärningsmän kunde få tag på personlig information från soptunnor eller genom att stjäla dokument under exempelvis inbrott (Wall, 2013 s. 439). Dock har teknikens framsteg gjort det möjligt för kriminella att få en global räckvidd. Personlig information kan därmed införskaffas mer effektivt med hjälp av datorer och en internetuppkoppling. Identitetskaparen kan komma åt viktig information som personnummer, passnummer, kontonummer, kreditkortsnummer, lösenord, telefonnummer, adresser och liknande. Denna information kan sedan användas för att bland annat öppna bankkonton, få kredit, köpa varor eller tjänster i offrens namn. Många av de individer samt

företag som fallit offer för identitetsstöld har drabbats av ekonomiska förluster, trakasserier från inkasserare och fordringsägare, avslag på ansökningar om lån, men även psykisk skada. En person vars identitet blivit stulen riskerar även att få ett "dåligt rykte", som följd av den brottsliga handlingen som begåtts i dennes namn. I många fall dröjer det ett tag innan offret upptäcker att hen utsatts för denna typ av brott. Detta kan i sin tur resultera i att det tar tid för den drabbade att "rensa" sitt namn samt betalningsanmärkningar som följd av det begångna brottet eller brotten. Ofta är personen som drabbats av identitetsstöld osäker och omedveten om hur dennes personuppgifter har stulits (Cassim, 2015 s. 73–75).

Identitetsstöld har blivit ett allvarligt och växande problem världen över. Detta då internets utveckling har lett till en ökad möjlighet för brottslingar att stjäla och olagligt använda personlig information för att begå bland annat identitetsstöld. Det som går att se är att identitetsstöld är en utmanande brottstyp att bekämpa för myndigheter och lagstiftare runt om i världen. Dessutom blir det mycket kostsamt för så väl staten som själva individen som utsatts för brottet, vilket även är problematiskt. Därför bör samhällsmedborgarna utbildas om riskerna som transaktioner online kan medföra, deras rättigheter när det gäller onlinebedrägerier samt åtgärder för att förebygga och hantera identitetsstöld. Därutöver bör även organisationer och internetleverantörer utbilda användarna om säker surfing eller erbjuda säkerhetspaket för sina användare (Cassim, 2015 s. 95–96).

Ett annat sätt att begå nätbrott med hjälp av e-postmeddelanden är "phishing". Så kallat phishing är den mest använda tekniken och är beroende av vanliga former av kommunikation som e-post för att lura offret att avslöja personuppgifter, ekonomiska uppgifter och dylikt (Wall, 2013 s. 437). Phishing kännetecknas av urskillningslösa utskick av miljontals e-postmeddelanden till personer som utger sig vara från dennes bank, eller något annat välkänt företag. Innehållet i e-postmeddelandena har oftast en liknande jargong där de uppger att offrets konto på en viss sida har utsatts för en säkerhetsöverträdelse. De ber sedan personen att klicka på en bifogad länk och att sedan uppge sina personuppgifter. E-postmeddelanden som skickas ut är ofta skickligt utformade vilket får offren att tro på bluffen. De kan innehålla fraser som "*efter olagliga försök att logga in på din banks webbplats ber vi dig att bekräfta din personliga information*", vilket leder till att uppgifterna hamnar i fel händer (Wall, 2013 s. 439). Det är även ett sofistikerat sätt att lura offren genom att skicka ut förfalskade webblänkar som är infekterade med virus. Klickar användaren på denna länk är det en falsk sida som dyker upp, vilket i sin tur smittar datorn med virus. Detta kan sedan förstöra hårddisken och komma åt känsligt material som sedan gärningsmannen får i besittning. Ett exempel på ett sådant virus är det så kallade "Zeus". Zeus är en professionellt utvecklad mjukvara, även kallat program, som

hämtar upp känsligt material från offrets hårddisk. Det har en så kallad "attack funktion" där den söker igenom datorn efter användarens säkerhetsuppgifter som kontonummer, personuppgifter, användar ID och lösenord till diverse webbplatser och skickar sedan detta till gärningsmannen. Det sprids vanligtvis via e-post eller oäkta internetlänkar och drabbar framförallt företag men även privatpersoner. Det är svårt att identifiera då datorn vid första anblick ser ut som vanligt, och offret vet inte att hen drabbats och att dennes uppgifter har läckt ut (Wall, 2013 s. 440).

Böhme och Moore genomförde en studie där de samlade in data för att kunna kartlägga EU-medborgarnas erfarenhet samt oro av brottslighet på nätet. De undersökte faktorer som tidigare utsatthet för nätbrott, oro för att utsättas för nätbrott samt exponering för nyhetsinslag om nätbrott. I deras studie framgick det att personer som inte hört något om brottslighet på nätet via nyhetsinslag eller från bekanta var mer benägna att handla på nätet än de som hade kunskap om denna typ av brott. Böhme och Moore hävdar dock att betydligt fler individer blivit medvetna om hotet och riskerna att utsättas för nätbrott. Detta har lett till att en del människor känner sig tveksamma att surfa på nätet på grund av den upplevda risken för att utsättas för brott (2012, s. 1). Böhme och Moore fann bland annat att oro samt erfarenhet av nätbrott leder till minskad aktivitet på internet, och att de som uttryckt känsla av oro har påverkats starkare (2012, s. 9).

2.1 Risker med användande av sociala nätverkssajten Facebook

"*Vi delar med oss av personlig information till främlingar, och följderna av det går inte att förutse, egentligen är det rena vansinnet***"**

(*Facebook follies*, 2011)

I den amerikanska dokumentären *Facebook follies* (2011) lyfts en del missöden fram som drabbat människor som använt Facebook. Citatet ovan uttrycks av den svenska berättarrösten i dokumentären, vilket kan anses vara en intressant aspekt som lyfts fram. Dokumentären tar även upp de risker som finns när individer väljer att dela med sig av personuppgifter online. Dock arbetar Sophos, ett toppmodernt företag placerat i Abingdon, England med att förhindra dataintrång samt att sätta stopp för diverse datavirus. Graham Cluley, med titeln Computer Security Expert, är en av företagets teknikkonsulter och har som arbetsuppgift att granska nätverkssajten Facebook. Han lyfter fram följande: "*What most people don't understand about*

Facebook is that it is not being done for love, it's a business". Cluley förklarar att många användare inte ser de risker som finns genom att ladda upp sina privata uppgifter på nätverkssajten. Han lyfter fram att många användare anser att Facebook är en gratistjänst, vilket han menar är felaktigt då personer hela tiden förser Facebook med personuppgifter och på så sätt "betalar Facebook med data". Personuppgifter sparas i Facebooks databaser som de sedan kan sälja vidare till andra företag. Facebooks användare blir därmed produkten som Facebook producerar och säljer. På detta sätt kan människors personuppgifter lätt spridas på global nivå och även hamna i fel händer (*Facebook Follies*, 2011).

Dokumentären lyfter även fram att det har blivit allt vanligare att hackers stjäl människors identiteter via sociala nätverkssajter, framför allt för att tjäna pengar.
Clive Thompson, frilansjournalist som intervjuas i dokumentären, tar även upp följande:

"*It's a truth of human history that whenever a new technology comes along, one of the first people who are gonna exploit it are criminals, because it gives them a new way to reach into people's lives, to gull them, to dupe them, you saw that with e-mail you know, like scam e-mails, and now we are seeing that with Facebook*".
(*Thompson, Facebook follies, 2011*)

Ett exempel som lyfts fram från verkliga livet drabbade Bryan Rutberg, vars facebookkonto blev hackat av en obehörig. Det var hans dotter som märkte hur Rutbergs facebooksida uppdaterades med en text där det stod att han befann sig i en allvarlig fara. Många av Rutbergs vänner skickade därmed meddelande till honom via Facebook och frågade vad som hade hänt. Detta utnyttjade hackaren, genom att utge sig för att vara Bryan Rutberg, och svarade med att familjen hade varit med om ett väpnat rån i London och att de nu behövde pengar för att kunna ta sig hem. En av Rutbergs vänner erbjöd sig därmed att föra över 1200 amerikanska dollar (ca 10800 SEK) för att hjälpa familjen hem. Detta meddelandet gick dock direkt till hackaren, som angav kontouppgifter tillhörande sig själv och fick på så sätt tillgång till pengarna (*Facebook follies*, 2011). Detta är ett exempel på hur sociala medier som Facebook kan bidra till bedrägerier och identitetsstölder. För att ytterligare förtydliga riskerna med att använda Facebook går Cluley även så långt med att hävda följande:

"*Facebook is the fastest growing hotbed of computer crime that exists on the internet. There's more crime, spam, scams and malware taking place on Facebook than anywhere else, if you want to go into the cybercrime hub of the world right now, it's Facebook*"
(*Cluley, Facebook follies, 2011*)

Han menar därmed att Facebook är den plats i cyberspace där flest nätbrott begås just nu, framför allt i form av bedrägerier och utskick av virus (*Facebook follies*, 2011).

2.2 Nätbrott utifrån ett rättssociologiskt perspektiv

Stefan Larsson framför i sin artikel "*Digitaliseringens rättssociologi*" att internets framväxt har fått en stor samhällelig betydelse. Användning av internet är något som fått en stor spridning runt om i världen bland olika åldersgrupper. I dag utgör internet en viktig samhällsfunktion då det dagligen används för att utföra diverse tjänster och aktiviteter. Det kan vara allt ifrån att använda sociala nätverk för att kommunicera, handla diverse varor och tjänster samt sprida nyhetsflöden. Detta har väckt frågor inom rättssociologin då vi som människor kan ha svårt att förstå alla de rättsliga konsekvenser som kan komma att ske med internets framväxt (2014, s. 80–81). Brott på nätet är ett fenomen som växt fram och som är i ständig förändring. Då 89 procent av Sveriges befolkning är internetanvändare och 60 procent använder sig av smartphones ökar emellertid riskerna att utsättas för denna typ av brottslighet. Det har även visat på en förändring av beteende och normer som skiljer sig från nätet jämfört med det fysiska rummet (ibid.). Larsson lyfter även fram problematiken kring nya normer som framkommit på nätet. Detta kan förklaras genom att människors beteende och handlingar tidigare har styrts av rättsliga normer, med andra ord lagen, i den icke-virtuella världen. Dock har internets framväxt lett till nya "sociala rum" och "nätcommunities" i cyberspace och det har resulterat i nya beteendemönster, med andra ord normer. Dessa normer skapas i en icke-rumslig kontext, där geografiska gränser suddas ut och brottsliga handlingar kan få en ny form och utföras på en global nivå (Larsson, 2014 s. 81–82). Som nämnts ovan kan det därmed bli problematiskt för lagen att styra dessa nya handlings-och beteendemönster på nätet. Detta kan förklaras med Thomas Mathiesens redogörelse för den så kallade växelverkan som uppstår mellan rätten och samhället. Enligt Mathiesen kan både rätten påverka samhället och samhället påverka rätten. Detta går att se då lagens främsta uppgift är att förhindra oönskat beteende bland individer i samhället. I andra fall kan även sociala normer komma att upphöjas till rättsliga normer och då är det samhället som påverkat rätten till förändring (2010, s. 117–118). De gamla "traditionella" handlingsföreskrifter som skett i den icke virtuella världen har lättare kunnat styras med

lagstiftning. Dock uppstår ett problem då dessa nya normer som skapas på nätcommunites och i cyberspace, inte går att styra på samma sätt, framför allt då de sker på en global nivå samt av anonyma användare. Lagens möjligheter att styra människors beteende blir därmed begränsat.

Även Dahlstrand med Wigerfelt och Wigerfelt lyfter fram hur lagen och sociala normer samverkar för att påverka beteenden. De menar att sociala normer har en stor inverkan på hur lagen är formulerad, då lagen skapas för att spegla samhällets moral och värderingar. Även lagen kan ha som åsyftad funktion att ändra sociala normer i samhället genom att förbjuda ett visst beteende eller handling med lagstiftning (2015, s. 1859, Svensson & Dahlstrand, 2014 s. 5).

En annan problematik som sker på cyberspace är att risken för att upptäckas vid utförande av ett nätbrott är mycket mindre, bland annat på grund av anonymiteten. Detta kan därmed leda till att en person som överväger att begå en brottslig handling i relation till risken att ertappas, fällas och straffas, väljer att begå brott. Då risken att upptäckas i cyberspace är betydligt mindre än i det fysiska rummet. Den sanktionering som även uppstår bland medmänniskor kan även elimineras när brottet sker anonymt i cyberspace (Svensson & Dahlstrand, 2014 s. 5).

2.3 Reglering av internet

I de flesta staterna har synen på internetreglering förändrats väsentligt genom åren och som även skapat en växande politisk debatt om hur dessa regler utförs av stater runt om i världen. Palfray hävdar att det idag inte längre är en fråga om huruvida internet kan regleras, utan snarare hur det bör regleras och hur detta regelverk ska genomföras på ett så effektivt sätt som möjligt. Detta då onlineaktiviteten har blivit en del av människors vardag, och inte enbart något vi ägnar oss åt ibland (Palfrey, 2010 s. 991–993). Cyberspace kan tolkas som ett ”virtuellt rum” där frihet råder, och där ingen stat kan genomdriva lagar eller upprätthålla ordning. Detta skapat en del utmaningar vad gäller att styra samt reglera detta ”virtuella rum” och de aktivitet som sker i cyberspace. Cyberspace kan förklaras som ett ”icke territoriellt” område som skiljer sig från det fysiska rummet som omfattar luft, hav, land och där stater inom sin förmåga kan utöva suveränitet och verkställa lagar inom ett relativt väl definierat område (Lino, 2015 s. 87).

Onlinesamhällen på internet fungerar på samma sätt som samhällen i den fysiska världen, det vill säga att kontroll är nödvändigt för att skapa ett så funktionsfritt och fungerande samhälle som möjligt (Kokswijk, 2010 s. 239). I sin artikel lyfter Lino fram två skilda sidor på hur forskare väljer att hantera problematiken gällande hur reglering av cyberspace kan

genomföras. Den ena sidan hävdar att rättssystemet har misslyckats med att hantera cyberspace och förespråkar istället skapandet av nya regleringsformer som är anpassade till dess komplexitet. Medan den andra sidan, den mer traditionella, påstår att utmaningen gällande lagstiftning och cyberspace inte skiljer sig från andra områden i det fysiska rummet och som kan vara lika komplexa som reglering av cyberspace (Lino, 2015 s. 87). En del mer traditionella anhängare anser att en internetpolis hade varit den optimala lösningen för att förhindra social oordning på nätet, men Kokswijk hävdar att "*there can be order without law. Not only is legislation unnecessary for law, but law is unnecessary for order*". Citatet kan tolkas som att Kokswijk anser att det kan vara ordning och reda utan lagstiftning i ett onlinesamhälle, och att lagstiftning kan anses vara onödig för att upprätthålla social ordning i icke-fysiska samhällen. Han fortsätter även att lyfta fram att många människor finner grundsatsen "alla är ansedda att känna till lagen" som svår, då lagar kan vara problematiska att tolka och veta hur de skall efterlevas. Detta leder då till att individer hellre gärna faller tillbaka på normer som de är vana att följa och efterleva (Kokswijk, 2010 s. 239). Om individer agerar på detta sätt kan juridiska funktioner som regelbildning, verkställighet av lag och tvistlösning med hjälp av lag, istället ersättas med att personer agerar efter informella sociala normer som accepterats i onlinesamhället. Effekter av detta kan därmed vara att staten inte kan stifta och reglera lagar, då medborgarna kommer att ignorera dem (ibid.). Lino lyfter fram Johnson och Post som hävdar att cyberspace tillhör internetanvändarna och därför bör "*those who have defined and use online systems have interest in preventing the security of their electronic territory and in preventing crime*". De menar med andra ord att självreglering av cyberspace bör tillämpas av internetanvändarna själva (2015, s. 92).

Då utvecklingen av webbplatser för socialt nätverkande sker snabbt i denna högteknologiska värld har begreppet självreglering fått allt större betydelse och det är ett hett diskuterat ämne gällande cyberspace (Kokswijk, 2010 s. 239). Det diskuteras ifall statens lagstiftning kan täcka och "nå ut till" onlinesamhällen, eller om självreglering kan vara en potentiell lösning. Att stifta lagar är även ett tids-och resurskrävande uppdrag, som även kan anses vara problematiskt (ibid.). För att förtydliga innebörden av självreglering kan det förklaras som ett institutionellt arrangemang, där en organisation styr medlemmarnas beteende med hjälp av allmänt accepterade normer (Kokswijk, 2010 s. 240). Självreglering kan även exemplifieras på följande sätt. Ett onlinesamhälle eller en social nätverkssajt skapas först och främst av en så kallad utvecklare. Det är även utvecklaren som sätter upp de gränser och regler som användare skall följa i ett så kallat "användarvillkorskontrakt", som användaren skall läsa igenom och sedan klicka i att de accepterar. I detta kontrakt framgår de rättigheter och

skyldigheter som användarna måste efterleva, och detta kan alltså ses som ett exempel på självreglering inom ett visst socialt "nätverksområde" där lagstiftning kanske inte behövs tas till i första hand (ibid.).

"Internet governance" som det kallas i det engelska språket innebär en slags "internetstyrning". Cogburn med kollegor beskriver denna internetstyrning som en utformning och tillämpning av kollektiva policies för det globala internetsamhället (Cogburn, et al. 2005 s. 12). Mathiason lyfter fram att internets tidiga utvecklare skapade ett medium som var avsett för att bidra till kommunikationsmöjligheter mellan människor, och att det snabbt uppstod olika sätt att bete sig och olika sätt att interagera (2009, s. xiv). I takt med internets utveckling har det diskuterats vem som skall styra internet samt hur det skall göras (ibid.). Drezner menar även att regeringar och staters jurisdiktioner är geografiska, medan internet ej har några synliga gränser. Han fortsätter med att säga att sammandrabbningar mellan de två kommer minska vad enskilda länder kan göra för att upprätthålla styrning av internet (2004, s. 480). Drezner går även så långt med att uttrycka att internationella organisationer saknar befogenhet att styra cyberspace och att interstatliga avtal och beslut tar för lång tid gällande stiftande av nya regler, vilket blir problematiskt då internets utveckling sker i en otrolig hastighet. Han menar även att den öppna och globala karaktären hos internet gör det svårt att utforma och genomföra effektiva regelverk med hjälp av statliga tillvägagångssätt (2004, s. 481). Drezner nämner även ett uttalande av Nicholas Negroponte, cyberenthusiast samt grundare av Massachusetts Institute of Techonologys forskningslaboratorium, där han säger att "*The internet can not be regulated. It's not the laws that aren't relevant, it's the nation-state that is not relevant*" (ibid.). Negroponte argumenterar för att det krävs en hög och sammanhängande kunskap om hur internet skall regleras och styras mellan diverse organisationer. De som han framför allt lyfter fram är organisationer som the Internet Engineering Task Force (IETF), som är ett internationellt community med forskare, nätverksingenjörer och nätverkstekniker som arbetar med utvecklingen av internetarkitekturen. The Internet Society (ISOC), som är en global organisation som arbetar för att internet skall hållas öppet och definierat av dess användare, samt att främja internets framväxt och utveckling på global nivå. The Internet Corporation for Assigned Names and Numbers (ICANN), ansvarar för att underhålla och granska databaser relaterade till diverse områden på internet, vilket säkerställer nätets stabila och säkra funktion. Negroponte menar att det krävs ett samarbete mellan organisationer som dessa för att försöka reglera internet (Drezner, 2004 s. 481). På så sätt kan en så kallad internet governance, eller internetstyrning uppnås. Det är dock en otroligt svår uppgift då internet ständigt utvecklas och nya användningsområden uppstår (ibid.).

De Vey Mestdagh och Rijgersberg hävdar dock att internet kan betraktas som ett stort självreglerande system eftersom dess globala räckvidd inte gör någon organisation kraftfull nog att kontrollera internet i sin helhet (2010, s. 386). De menar även att interaktion på internet framförallt bygger på samspel mellan individer med gemensamma intressen. Den tekniska arkitekturen bidrar också till kunskap samt tekniska resurser för både enskilda internetanvändare men även större organisationer, detta kan i sin tur hindra stater från att få omfattande regleringsmöjligheter. Till följd av detta är staternas förmåga att kontrollera internet begränsat, vilket kan leda till en slags decentralisering av reglering (ibid.). Detta kan därmed förklaras som en slags självreglering av individerna själva eller av individer i mindre grupper, vilket De Vey Mestagh och Rijgersberg har valt att benämna som "*original self regulation*" (2010, s. 387). Ju fler människor som involveras i dessa grupper desto komplexare blir samarbetet mellan dem och det kan därmed underlätta att delegera regleringsbefogenheter inom grupper. Denna delegation delas upp i tre olika typer som De Vey Mestagh och Rijgersberg titulerar för "*coordinate*", "*superordinate*" och "*subordinate*". Delegeringen sker på följande sätt, en grupp delar upp sina delegeringsbefogenheter till en delgrupp inom gruppen för att samordna beteendet och på sätt uppstår egna sociala normer och beteendemönster (ibid.). Den så kallade coordinate delegering är mycket vanligt och bevarar den självreglerande karaktären av den ursprungliga sorten av självreglering, med andra ord "*original self regulation*". För att exemplifiera denna uppdelning som exempelvis sker i diverse organisationer tillsätts ett antal komittéer. Det kan exempelvis vara systemadministratörer som sköter regleringen på diverse sociala nätverkssajter (ibid.). Superordinate delegering innebär att större organisationer som exempelvis ICANN, som arbetar för att försöka reglera internetanvändarna i så stor utsträckning som möjligt. Den sista så kallade subordinate delegeringen avser staters begränsade förmåga att skapa regleringar i ett försök att styra individers beteenden online. Då stater har mer makt och befogenhet att reglera människors beteende i det fysiska rummet kan de därmed anses som underordnade när de försöker reglera beteenden i cyberspace (De Vey Mestagh & Rijgersberg, 2010 s. 388). De Vey Mestagh och Rijgersberg försöker med detta förklara hur självreglering av internet kan fungera i form av grupper och organisationer när statens befogenhet begränsas.

För att därmed koppla rättssociologi till det rådande problemområdet går det att argumentera för att staten och lagstiftarna inte har den möjlighet och makt att reglera samhällsmedborgarna i cyberspace som de har i det fysiska rummet. Detta då beteendemönster online har ändrats väsentligt på grund av den högteknologiska utvecklingen. Som nämnts ovan

är individer idag anonyma och brottslighet kan begås på en global nivå, vilket gör det svårt för lagstiftarna att reglera människors beteende.

2.4 Vad säger lagen?

I svensk lagstiftning finns det för närvarande endast två definierade lagar som uttryckligen omfattar nätbrott. De tas upp i Brottsbalken 4 kap. 9 c § rörande dataintrång samt 9 kap. 1 § andra stycket gällande datorbedrägeri. I Brottsbalken 4 kap. 9 c § framgår följande:

"*Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.*

Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art.
(SFS 2014:302).

Lagen 9 kap. 1 § andra stycket i brottsbalken gällande datorbedrägeri lyder som följande:

"För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan.
(SFS 1986:123)."

Svensson och Dahlstrand pekar på att informationstekniken inte medfört några större förändringar i lagstiftningen utifrån ett rättsligt perspektiv. Detta då det fortfarande finns en avsaknad av lagar som specifikt reglerar diverse brott som sker på nätet. Istället tillämpas lagar som omfattar traditionella brott och som bland annat utgörs av ofredandebrotten, olaga hot eller ärekränkningsbrotten, detta även inom sociala medier (2014, s. 24). Det finns även andra brott som täcks under gällande lagstiftning, exempelvis hamnar phishing under bedrägeri som berörs under Brottsbalkens 9:de kapitel (*Polisen*, 2017). Även personuppgiftslagen (PUL) tillämpas ofta till brott som begås på nätet gällande identitet, integritet samt personuppgifter. Till PUL

räknas all den information som antingen kan kopplas indirekt eller direkt till en fysisk person som är vid liv. Information som räknas som personuppgift och därmed omfattas av PUL är, namn, personnummer, kundnummer samt foton (ibid.). Dock saknas det särskilda lagar som specifikt reglerar publicering som sker på internet. Det finns enbart generella regler som omfattar hantering av personuppgifter och som även täcker personuppgifter som publiceras på diverse webbsidor samt bloggar (*Datainspektionen*, 2017). Enligt PUL är även sociala medier som Facebook, Twitter eller Instagram tvungna att förhålla sig till denna lag, detta då de hanterar människors personliga uppgifter (ibid.).

Det som dock bör uppmärksammas och som Enarsson lyfter fram är att det finns en risk för en övertro till lagstiftning och vad nya lagstiftningsåtgärder gällande nätbrott kan bidra med. Att stifta en ny lag behöver inte nödvändigtvis innebära en lösning på problemet, det krävs även att lagen omsätts i det praktiska och inte enbart i teorin. Skulle eventuellt en ny lagstiftning som utformats med hänsyn till den tekniska utvecklingen inte fungera i praktiken, finns det en risk för att enskilda förlorar tilltro till rättsväsendet. Vilket i sin tur kan resultera i att det blir svårare att både utreda men även bekämpa denna typ av brottslighet för rättsväsendet. Denna tekniska utveckling som internet medfört kräver därmed inte enbart en väl utformad lagstiftning, utan även ett rättsväsende med hög kompetens i hur den rättsliga samt tekniska utmaning som samhället befinner sig i skall hanteras (Enarsson, 2015).

3. Teoretiskt ramverk

3.1 Risksamhälle och risker online

Enligt Ulrich Beck är begreppet risk en social konstruktion, vilket innebär att när människor interagerar med varandra kan risker uppkomma till följd av detta. Det kan även förklaras som en framtida händelse, där förstörelse eller något annat negativt inte har hänt än. Detta kan komma att få ett negativt utfall, ifall en individ väljer att utföra en viss handling (McDonald & Lang, 2014 s. 128). Enligt vetenskaplig forskning framgår det dock att det inte finns någon universell uppfattning om begreppet risk. Det finns ett brett spektrum av åsikter gällande innebörden av risk och risktagande. Det innebär alltså att det skiljer sig från individ till individ om vad man anser vara en farlig situation eller ej. Detta beror även helt på en individs riskuppfattning samt risktolerans (Inouye, 2014 s. 2). Beck hävdar även att en individs kunskap och medvetenhet är avgörande i riskbedömningen av ett hot. Detta då en person som saknar kunskap inte kan definiera en potentiell risk och riskerar därmed att utsättas sig för en negativ händelse (2000, s. 74–75). I ett närmre försök att definiera risk kan det beskrivas som ett sätt

att mäta och försöka förutspå sannolikheten för att en händelse skall få ett negativt utfall. Med andra ord kan risken vara en beräkning av hur sannolikt det är att en incident skall ske, samt hur följderna kan bli (Inouye, 2014 s. 2).

Den tyske sociologen Ulrich Beck myntade begreppet samt teorin "risksamhälle" då han redogör för diverse risker som ett samhälle kan utsättas för. Beck gör en distinktion mellan vad han kallar för ”externa risker” och ”tillverkade risker”. De externa riskerna fanns i det klassiska industrisamhället och förknippades med naturen, till exempel infektionssjukdomar, dålig skörd och naturkatastrofer i form av översvämningar. Medan de tillverkade riskerna skapas som en effekt av vår utvecklade kunskap om världen. Med andra ord en konsekvensens av mänskliga handlingar, ett resultat av vetenskaplig och teknisk utveckling som omfattar nya risker som global uppvärmning, kärnkraftsvapen, genmanipulation eller missbruk av internetanvändande. Risker har därmed alltid funnits med en skillnad att de inte längre kommer ”utifrån” utan från människan själv, då individer skapat dessa risker (Beck, 2000 s. 33, Newburn, 2013 s. 901–902). Den tekniska och ekonomiska utvecklingen i det moderna samhället har skapat nya risker, vilket är en konsekvens av moderniseringen (Beck, 2000 s. 52).

Marko Eskola hävdar bland annat att det moderna informationssamhället vi lever i har blivit ett nytt ”risksamhälle”, vilket ger stöd i Becks teori om ett så kallat risksamhälle. Eskola menar att nya globala risker skapats i samband med information- och kommunikationstekniken framväxt. Då denna utvecklingen kan ses ha gett upphov till nya risker i form av exempelvis nätbrottslighet, var syftet nödvändigtvis inte att skada samhället utan snarare gynna det. Därmed kan nätbrott förklaras som en “bieffekt” av denna utveckling som uppstått på grund av bristande kunskap hos människan. Eskola refererar till Beck som hävdar att risker uppstår på grund av att människor utvecklat en teknik som de inte haft tillräckligt med kunskap om samt vilka konsekvenser den kan komma att få (2012, s. 122–124). Vidare hävdar Beck att människor tenderar att ha för mycket tillit till forskare och organisation som arbetar med teknik och information (Eskola, 2012 s. 131).

Även Oweis med kollegor hävdar att det finns risker i samband med internetanvändning. De lyfter fram att internetanvändare riskerar att utsättas för hacking och att personuppgifter läcks ut och sprids via sociala nätverkssajter. Det är framför allt personuppgifter som namn, födelsedatum, adress och bilder som riskerar att spridas och hamna i fel händer. Detta kan ske då många personer använder sig av sociala nätverkssajter för att dela med sig av information och bilder som laddas upp och sparas i cyberspace (Oweis, et al. 2014 s. 3). Att samtala online i diverse chattforum medför även en del risker. Exempelvis kan individer helt anonymt kontakta varandra från alla delar av världen. Oweis med kollegor menar att unga lätt blir naiva och delar

med sig av personlig information, ovetande om vem som sitter på andra sidan av datorskärmen. På så sätt kan även känslig information spridas och brukas för kriminella handlingar. Personuppgifter som vanligtvis sprids via chattforum är telefonnummer, e-mail adresser och vart en individ befinner sig rent geografiskt (ibid.).

Ett stort problem som uppstår gällande nätbrott är att det kan få en global omfattning, eftersom internet ger människor möjligheten att begå brott från olika delar av världen. Vidare hävdar Eskola att det krävs mer resurser för att effektivisera det brottsförebyggande arbetet mot cybercrime. Emellertid går det att se att det ofta saknas tillräckligt med kunskap samt kvalificerad personal inom de olika brottsförebyggande organisationerna, vilket försvårar arbetet mot nätbrott. Därför krävs det ett bättre samarbete mellan olika organ, på så väl nationellt som internationellt plan, för att kunna tillhandahålla den kunskap som krävs för enskilda organisationer men även för att effektivisera det brottsförebyggande arbetet (Eskola, 2012 s. 134, 141). Även anonymitet är något som berörs av Eskola som menar att anonymiteten på internet är mycket problematiskt då det utgör ett hot och en stor utmaning för säkerheten i cyberspace (2012, s. 133).

3.2 Kritik mot Becks teori om risksamhället

En del kritik har riktats mot Ulrich Becks teori gällande risksamhället. Rosborg lyfter fram att Becks teori kan antas vara generaliserande och spekulativ då han saknar dokumentation samt empiri i det han påstår gällande risksamhället. En annan kritik som lyfts fram mot Beck är att han enbart belyser negativa aspekter med risker och att han bortser från att det faktiskt existerar positiva aspekter med risker. Rosborg menar att det krävs ett visst risktagande för att nå ekonomisk framgång i samhället, för att utveckla teknologin samt vetenskapen och att risker därmed kan anses som positiva. Ytterligare kritik som riktas mot Becks teori om risksamhället är att han sammanfattar de nutida samhället enbart utifrån risker, vilket kan anses vara generaliserande. Han belyser därmed ej andra aspekter som kan påverka ett samhälle som exempelvis media. Rosborg fortsätter med att redogöra för att människor utsätts för medias överdrivna spegling av kriminalitet och våld, vilket skulle innebära att vi snarare lever i en rädslokultur än i ett risksamhälle (Rosborg i Andersen och Kaspersen, 2007 s. 359–360).

4. Metod och genomförande

För att undersöka medvetenheten för att utsättas för brott på nätet och de risker som finns gällande identitet, integritet och personuppgifter konstruerades ett frågeformulär bestående av

ett 20-tal frågor. Det material som delades ut till studiens undersökningsobjekt bestod av en enkät som delades ut både som webbenkät via Facebook samt i pappersform. Enkäten bestod av sju sidor inklusive ett försättsblad med instruktioner. Respondenterna fick besvara totalt 22 frågor exklusive kön och ålder. 18 av frågorna var konstruerade med svarsalternativ där respondenterna fick ringa in ett svarsalternativ, förutom fråga 13 där respondenten ombads fylla i två svar. Anledningen till detta var att en bredare kunskap eftersöktes gällande vilken brottstyp unga vuxna är mest oroliga för. Respondenterna ombads även att besvara fyra öppna kvalitativa frågor, där de fick möjligheten att utveckla sina svar. Detta för att nå en djupare kunskap och förståelse gällande respondenternas attityder, kunskap samt medvetenhet kring ämnet.

4.1 Val av frågor till respondenter

För att kunna få en allmän bild om hur unga vuxna använder internet och hur ofta de gör det ställdes frågorna ett och två. Fråga tre till åtta ställdes i syfte för att kunna besvara frågan gällande hur medvetna unga vuxna är om de risker som finns på nätet gällande integritet och personuppgifter. Detta för att även eftersöka ifall deras kunskap eller också okunskap påverkar deras internetanvändande samt risktagande online. Fråga nio och tio ställdes för att undersöka ifall unga vuxna känner oro för att utsättas för brott på nätet samt vad denna möjliga oro beror på. Fråga elva ställdes till respondenterna för att få en bild av vilken typ av nätbrott unga vuxna är mest oroliga att utsättas för. Ytterligare frågor gällande unga vuxnas kunskap ställdes i fråga tolv där respondenterna fick svara på hur de skyddar sig mot diverse brott på nätet. Detta för att undersöka ifall unga vuxna har den kunskap som krävs för att kunna skydda sig i så stor utsträckning som möjligt mot nätbrott. I fråga 13 fick respondenterna besvara vart eller från vem de fått kunskap ifrån gällande brott på nätet. Detta för att få en bild över vilka informationskällor som är de mest effektiva i att nå ut till unga vuxna. Frågorna 14, 15 och 16 utformades för att ytterligare få en bild av vilken kunskap unga vuxna har gällande hur de aktivt utför diverse åtgärder för att minska risken för att utsättas för brott på nätet. Det var även av intresse att undersöka ifall unga vuxnas kunskap samt medvetenhet kring risker online påverkar deras trygghetskänsla och därav ställdes fråga 17. För att kunna besvara frågan om vilken attityd unga vuxna har till lagstiftningen och dess möjligheter att påverka nätbrott ställdes fråga 18 till 21. Detta för att undersöka hur medvetna unga vuxna är kring lagstiftningen gällande brott på nätet. Det eftersöktes även svar på hur stor tilltro unga vuxna har till lagstiftningens möjlighet att skydda medborgarna från att utsättas för nätbrott, samt ifall de tror att lagstiftning kan förhindra att brott begås på nätet. Ifall de ansåg att lagstiftningen ej kan förhindra nätbrott

ombads respondenterna utveckla sitt svar. För att få en helhetsbild av unga vuxnas förtroende för rättsväsendets, det vill säga polis, Sveriges domstolar samt brottsförebyggande myndigheters förmåga att förhindra nätbrott ställdes fråga 22. Onumrerade frågor ställdes på sista sidan för att få en överblick av respondenternas kön samt ålder. För att dra en koppling till den valda teorin om risksamhället och de risker som uppstår online går det att knyta an till Becks begrepp om tillverkade risker. Det kan argumenteras för att människor i dagens högteknologiska värld är omedvetna när de använder sig av internet och att de ej besitter nog med kunskap om de risker som finns online. På så sätt skapar individer egna risker, med andra ord tillverkade risker, en konsekvens av den tekniska utvecklingen samt människors handlande (Beck, 2000 s. 33, Newburn, 2013 s. 901-902).

4.2 Webbenkät

Det första steget i studien var att testa enkätundersökningen, den publicerades därmed som webbenkät på våra personliga facebookkonton. Det var ett effektivt sätt att nå ut till unga vuxna internetanvändare för att snabbt få in svar. Under de första 24 timmarna hade 46 stycken respondenter besvarat enkäten och efter ytterligare två dygn hade totalt 55 personer svarat. Något som även effektiviserade datainsamlingen som gjordes via webbenkäter var att när frågorna besvarades via hemsidan matades datan in per automatik och framställdes sedan i cirkeldiagram. Ett problem som dock uppstod var att alla respondenter inte svarade på alla frågor. På www.webbenkäter.se går det att se hur många som svarat på respektive fråga, samt vilka hen har valt att hoppa över. Det gick dock inte att identifiera vilken person som valt att avstå från att besvara en viss fråga. Det gick därmed ej att utesluta de enkäterna som ej var korrekt besvarade, valet blev därmed att helt och hållet utesluta webbenkäter från denna studien och istället gå ut på campusområden i Lund och dela ut enkäterna fysiskt i pappersform. Därmed trycktes enkätundersökningen ut i pappersform och delades sedan ut till helt nya respondenter som kommer vidare att beröras under 4.3 och 4.4.

4. 3 Enkäter i pappersform

Samtliga 108 enkäter delades ut mellan onsdagen den 19:e och torsdagen den 20:e april 2017 på diverse universitetsområden i Lund. Anledningen till att 108 enkäter valdes att tryckas ut berodde på att målet var att samla in ett hundratal enkäter. Detta för att stärka studiens reliabilitet, då ett högre antal insamlade svar ger en ökad tillförlitlighet till studien (Bryman,

2008 s. 49). Enkäterna delades ut till deltagarna av författarna själva. Utdelning av enkäterna gick till på följande sätt, undersökningsledaren närmade sig en potentiell deltagare genom att kortfattat berätta om undersökningen, samt fråga ifall personen kunde tänka sig att medverka. Vid samtycke tilldelades personen en enkät som tog cirka tre till fem minuter att besvara. Under tiden som enkäten fylldes i av deltagaren distanserade sig undersökningsledarna fysiskt från deltagaren för att undvika känslor av stress eller övervakning. Undersökningsledarna övervakade dock processen på avstånd för att bedöma om deltagaren var färdig. När deltagaren var färdig tackades denne för sitt medverkande och enkäten samlades in. Efter insamlat material räknades enkäterna och en granskning av data gjordes i sökande av fullständigt ifyllda enkäter. Av de 108 utdelade enkäterna ansågs 97 som korrekt ifyllda. Elva enkäter fick uteslutas och anses som bortfall då fem av dessa hade besvarats av personer över 30 års ålder. Då studien riktar sig till unga vuxna och indelningarna av åldersgrupper endast sträcker sig till 30 år fick dessa därmed uteslutas. I de resterande sex enkäterna hade respondenterna ej besvarat fråga 16 och 17, och fick därmed uteslutas på grund av ofullständiga uppgifter. Kategoriseringen av data gjordes manuellt där enkäterna granskades och räknades på följande sätt. I det första steget undersöktes respondenternas ålder samt kön. Åldersgrupperna delades in i tre kategorier, under 20 år, 20–25 år samt 26–30 år. Beroende på vad respondenten svarat delades enkäterna upp i respektive åldersgrupp för att kunna räkna in antalet respondenter i varje grupp. Även kön kategoriseras och räknades in likadant, där en uppdelning av kvinna, man och annat gjordes. Därefter granskades varje fråga i enkäten och en uppdelning i olika grupper gjordes beroende på vilket svarsalternativ respondenten valt. Detta för att kunna framställa datan i diagram genom användning av datorprogrammen Excel och Numbers. Slutligen genomfördes en innehållsanalys och tolkning av de öppna frågorna genom en kategorisering av begrepp och förklaringar som respondenterna uppgav. Detta för att få fram genomgående teman, mönster och samband i respondenternas svar, som sedan redovisas under analys och diskussion (Denscombe, 2009 s. 373–374).

4.4 Undersökningsdeltagare

I enkäten som trycktes ut i pappersform deltog 97 personer. De valdes ut genom ett slumpmässigt urval inom vår valda population bestående av unga vuxna. Detta tillvägagångssätt innebär att respondenter väljs ut av undersökningsledaren slumpartat för att få ett så representativt tvärsnitt av den valda populationen som möjligt (Denscombe, 2009 s. 33). Majoriteten av studiens deltagare var 20–25 år och könsfördelningen var 39 män och 56 kvinnor. Variabeln ”annat” fanns även med under kategorin ”kön”. Detta för att undvika att

individer som ej identifierar sig med något av de traditionella könen avstår från att besvara frågan gällande kön. Två personer identifierade sig som "annat" inom kategorin kön. Studiens deltagare kan även antas tillhöra gruppen unga vuxna som är studenter vid Lunds universitet. Detta då enkäterna delades ut bland unga vuxna i miljöer som tillhör Lunds universitetet. Enkäterna delades ut på platser som Eden, Rättssociologiska institutionen, LUX och LTH i Lunds stad.

4. 5 För-och nackdelar med kvantitativ metod

Valet av kvantitativ metod gjordes för att nå ett så brett antal respondenter som möjligt och det är även en effektiv metod när forskaren är tidsbegränsad. Det finns ytterligare fördelar med denna typ av metod, en ekonomisk fördel är att materialet i form av pappersenkäter kostar relativt lite att framställa. Det är även lättare att genomföra en kvantitativ undersökning jämfört med intervjuer, då det kan vara svårare att finna lämpliga person som dessutom är villiga att delta i studien (Denscombe, 2009 s. 225-226). Detta var en av orsakerna till att den kvantitativa metoden valdes att tillämpas. En annan stor fördel som vi fann med att dela ut enkäter i pappersform, var den personliga kontakten med respondenterna. Vi som forskare fick en möjlighet att presentera och förklara vårt arbete och svara på eventuella frågor gällande enkäten. Vi fann även att en större del av respondenterna svarade i mycket större utsträckning på frågorna när forskaren befann sig i närheten. Det är även en undersökningsmetod som går att generalisera i större utsträckning beroende på hur många respondenter som deltagit (Denscombe, 2009 s. 55). Även replikerbarheten ökar då andra forskare kan utföra studien på ett liknande sätt och kan eventuellt nå fram till samma resultat (Bryman, 2008 s. 49). En av nackdelarna med att välja kvantitativ metod är att forskaren inte får samma djup genom att ställa frågor via enkätundersökningar. Detta då forskaren inte har samma möjlighet som vid en intervju att be respondenten utveckla svaret ytterligare (Denscombe, 2009 s. 56). Av den anledning valdes ett antal öppna frågor för att försöka nå en bättre förståelse och kunskap kring vissa frågor Det var dock problematisk när ett antal deltagare hoppade över de öppna frågorna, och enkäterna fick uteslutas som bortfall. En annan problematik som kan uppstå är när forskaren skall mata in data i uträkningsprogram som Excel. Detta då forskaren kan råka begå misstag vid manuell inmatning av data. Därav är det viktigt att data som matas in, kontrolleras av forskaren mer än en gång. Detta för att minimera risken för att missvisande data skall framställas (Denscombe, 2009 s. 226).

4.6 Resultat av enkätundersökning

Denna studie ämnar att undersöka hur medvetna unga vuxna är om de risker som finns gällande nätbrott och internetanvändning. Syftet med studien var även att undersöka vilken kunskap samt attityd unga vuxna har till lagstiftningens möjligheter att påverka nätbrott. Nedan presenteras respondenternas svar på varje fråga i enkätundersökningen i form av cirkeldiagram.

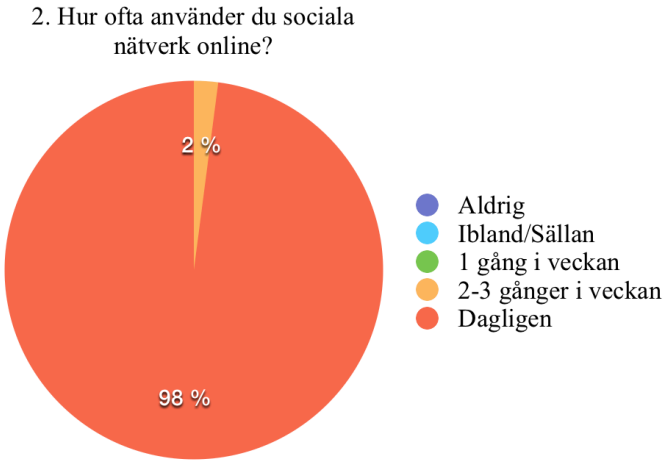
Fråga 1. *Har du ett konto på något socialt nätverk online?*

Samtliga 97 deltagare (100 procent) angav att de har något socialt nätverk online, se figur 1.

Figur 1.

Fråga 2. *Hur ofta använder du sociala nätverk online?*

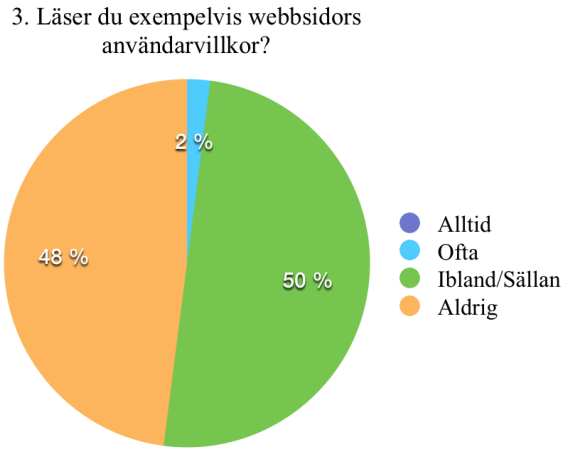
95 deltagare (98 procent) uppgav att de använder sig av internet dagligen. Två av deltagarna (två procent) uppgav sig använda internet två till tre gånger i veckan.



Figur 2.

Fråga 3. *Läser du exempelvis webbsidors användarvillkor?*

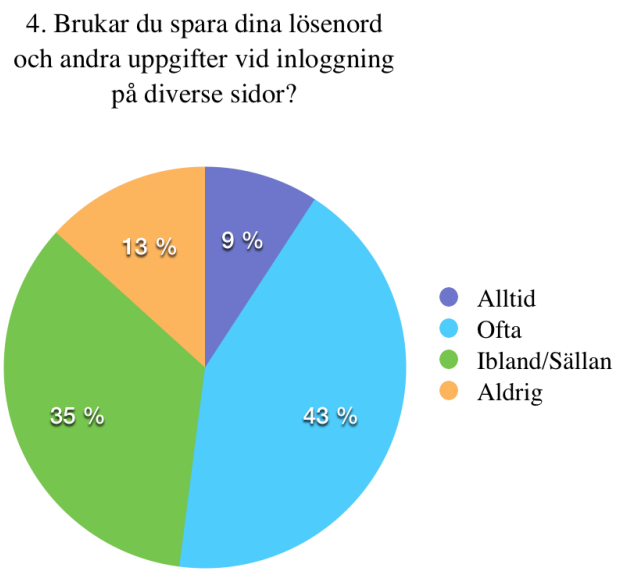
47 av deltagarna (48 procent) angav att de aldrig läser webbsidors användarvillkor. 48 av deltagarna (50 procent) angav att de ibland/sällan läser webbsidors användar villkor och endast två deltagare (två procent) angav att de ofta läser användarvillkoren.



Figur 3.

Fråga 4. *Brukar du spara dina lösenord och andra uppgifter vid inloggning på diverse sidor?*

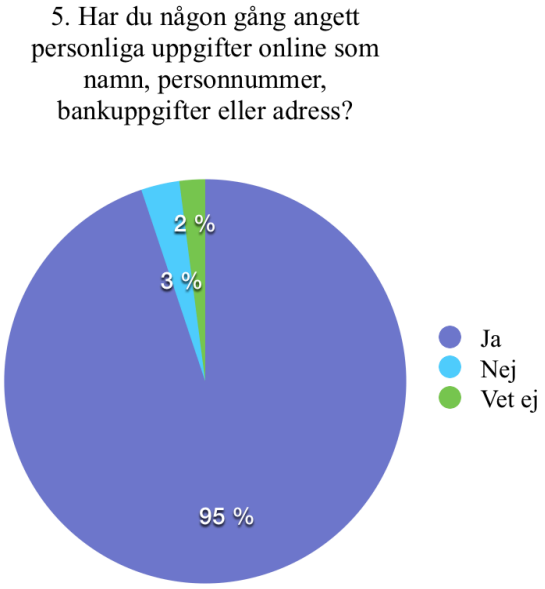
Tolv av deltagarna (13 procent) uppgav att de aldrig sparar sina lösenord eller andra uppgifter vid inloggning på diverse online sidor. 34 deltagare (35 procent) uppgav att de ibland/sällan sparar dessa uppgifter. 42 deltagare (43 procent) uppgav att de ofta sparar sina lösenord eller andra uppgifter och endast nio deltagare (nio procent) uppgav att de alltid sparar sina uppgifter på diverse online sidor.



Figur 4.

Fråga 5. *Har du någon gång angett personliga uppgifter online som namn, personnummer, bankuppgifter eller adress?*

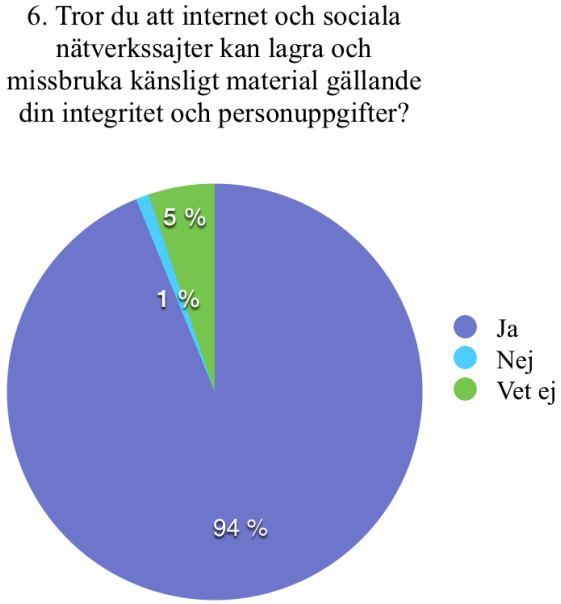
92 deltagare (95 procent) uppgav att de någon gång uppgett personliga uppgifter på nätet. Tre deltagare (tre procent) uppgav att de inte uppgett personliga uppgifter och två deltagare (två procent) uppgav att de inte vet.



Figur 5.

Fråga 6. *Tror du att internet och sociala nätverkssajter kan lagra och missbruka känsligt material gällande din integritet och personuppgifter?*

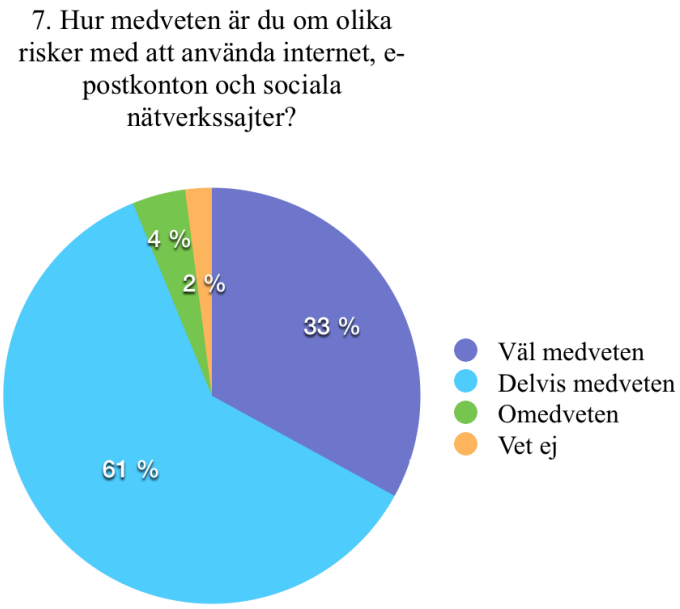
91 av deltagarna (94 procent) anser att såväl internet som diverse sociala nätverkssajter kan lagra och missbruka deras personliga uppgifter. Endast en deltagare (en procent) uppgav att hen inte tror att denna typ av material kan lagras och missbrukas. Fem deltagare (fem procent) uppgav att de inte vet ifall känsligt material på nätet kan lagras och missbrukas.



Figur 6.

Fråga 7. *Hur medveten är du om olika risker med att använda internet, e-postkonton och sociala nätverkssajter?*

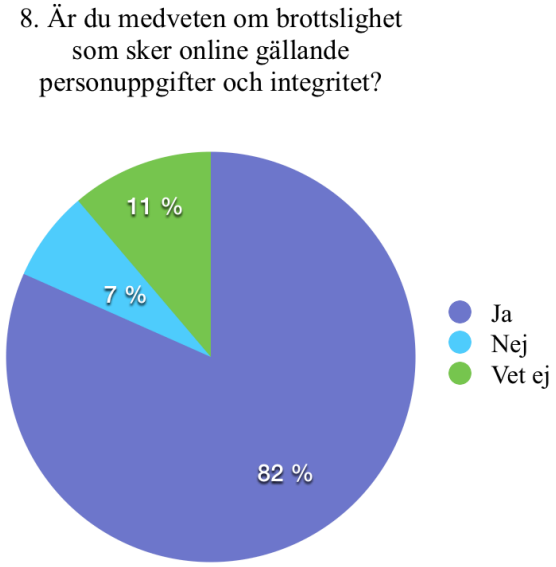
32 deltagare (33 procent) uppgav att de är väl medvetna om de risker som finns med internetanvändande. 59 deltagare (61 procent) uppgav att de är delvis medvetna om de risker som finns. Fyra deltagare (fyra procent) uppgav att de är omedvetna om riskerna på nätet och endast två deltagare (två procent) uppgav att de ej vet något riskerna.



Figur 7.

Fråga 8. *Är du medveten om brottslighet som sker online gällande personuppgifter och integritet?*

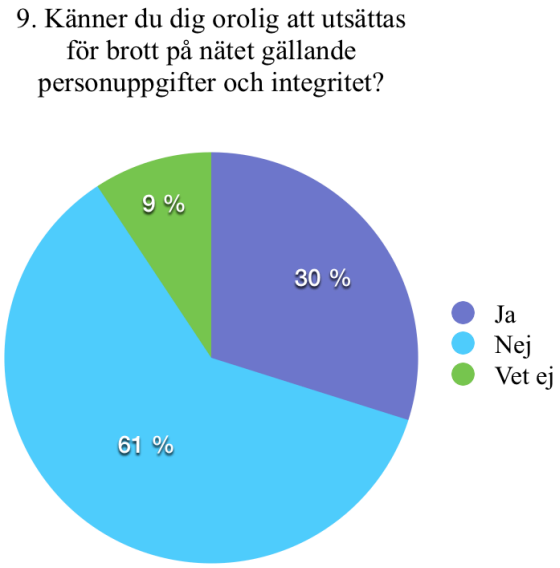
79 deltagare (82 procent) uppgav att de är medvetna om brottsligheten som sker online gällande personuppgifter och integritet. Sju deltagare (sju procent) uppgav att de inte är medvetna om brottsligheten som sker online. Elva deltagare (elva procent) uppgav att de inte kan bedöma sin medvetenhet kring denna typ av brottslighet.



Figur 8.

Fråga 9. *Känner du dig orolig att utsättas för brott på nätet gällande personuppgifter och integritet?*

29 deltagare (30 procent) uppgav att de känner sig oroliga för att utsättas för brott på nätet gällande personuppgifter och integritet. 59 deltagare (61 procent) uppgav att de ej känner sig oroliga för att utsättas för denna typ av brott. Nio deltagare (nio procent) uppgav att de ej kan bedöma sin oroskänsla.



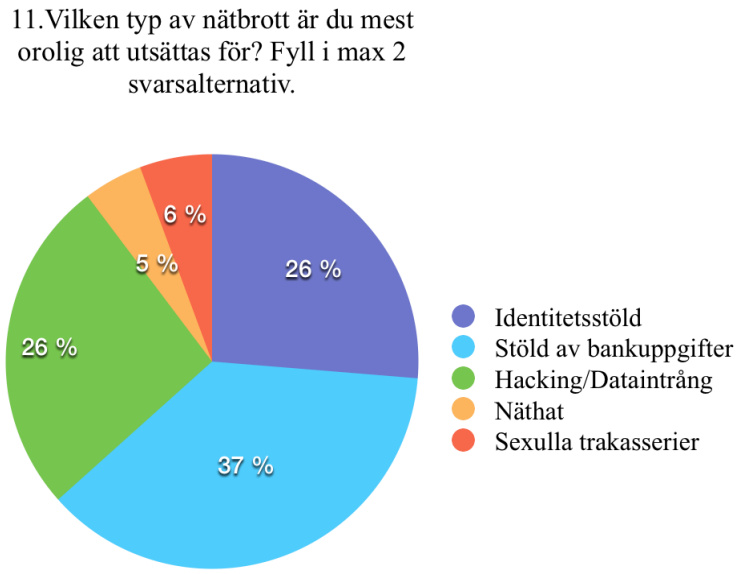
Figur 9.

Fråga 10. *Om ja, vad orsakar denna oro?*

I den här frågan ombads respondenterna som uppgett att de känner sig oroliga för att utsättas för brott på nätet gällande personuppgifter och integritet att utveckla orsaken till detta. 30 deltagare besvarade fråga tio med ett kvalitativt svar i form av skriven text. Varav 29 deltagare uppgett i fråga nio att de känner sig oroliga och en deltagare som uppgett att denne ej vet, men som ändå valt att besvara fråga tio. För att tolka respondenternas svar gjordes en kvalitativ innehållsanalys i ett sökande för att finna genomgående teman samt begrepp i svaren (Bryman, 2008 s. 243, Denscombe, 2009 s. 307). I en granskning av den öppna frågan, gjordes ett kodningsschema för att kunna finna ett genomgående tema i de olika svaren från respondenterna. Exempelvis lades fem deltagares svar ihop i samma kategori, då de nämnde att de hört berättelser där andra blivit offer för nätbrott via bekanta eller media, vilket skapat en oroskänsla. Två deltagare uppgav att de inte har tillräckligt med kunskap om hur de skall skydda sig mot denna typ av brott på nätet. Fyra deltagare uppgav att de finner svårigheter i att skydda

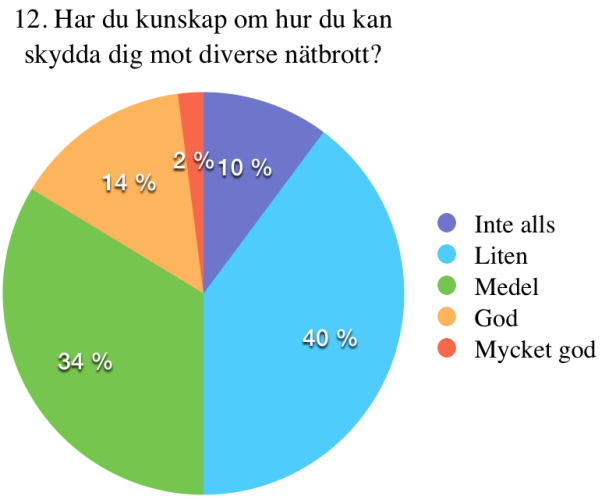
sig mot nätbrott. 13 deltagare uppgav att de känner sig oroliga för att känsligt material i form av exempelvis bankuppgifter skall hamna i fel händer och därmed även missbrukas. Tre deltagare uppgav att allt fler individer använder internet och att därmed kunskapen ökar om hur känsligt material kan missbrukas. Tre deltagare uppgav även att de känner oro för att bli offer för identitetsstöld.

Fråga 11. *Vilken typ av nätbrott är du mest orolig att utsättas för?*
51 deltagare (26 procent) uppgav att de är oroliga för att utsättas för identitetsstöld. 72 deltagare (37 procent) uppgav att de är oroliga för att utsättas för stöld av bankuppgifter. 51 deltagare (26 procent) uppgav att de är oroliga för att utsättas för hacking eller dataintrång. Nio deltagare (fem procent) uppgav att de är oroliga för näthat och elva (sex procent) uppgav att de är oroliga för att utsättas för sexuella trakasserier.



Figur 11.

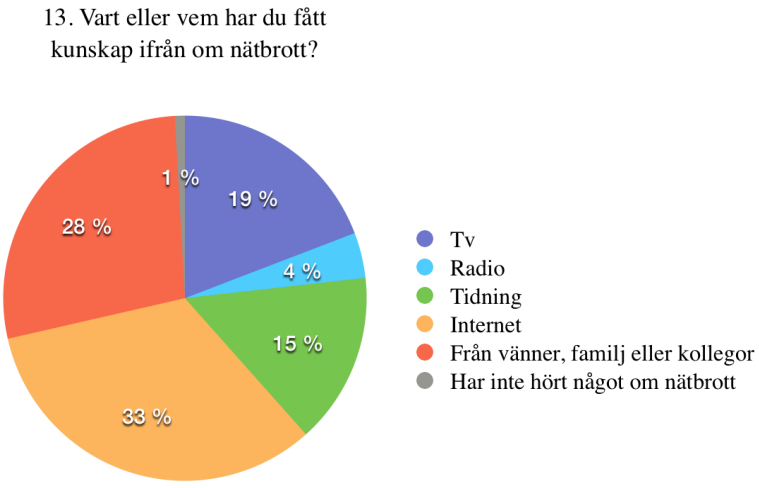
Fråga 12. *Har du kunskap om hur du kan skydda dig mot diverse nätbrott?*
Tio deltagare (tio procent) uppgav att de inte har någon kunskap alls om hur de skall skydda sig mot diverse nätbrott. 39 deltagare (40 procent) uppgav att de har en liten kunskap om hur de skall skydda sig mot nätbrott. 33 deltagare (34 procent) uppgav att de har en medel kunskap om hur de skall skydda sig. 13 deltagare (14 procent) uppgav att de har en god kunskap om hur de skall skydda sig och endast två deltagare (två procent) ansågs ha en mycket god kunskap.



Figur 12.

Fråga 13. *Vart eller vem har du fått kunskap ifrån om nätbrott?*

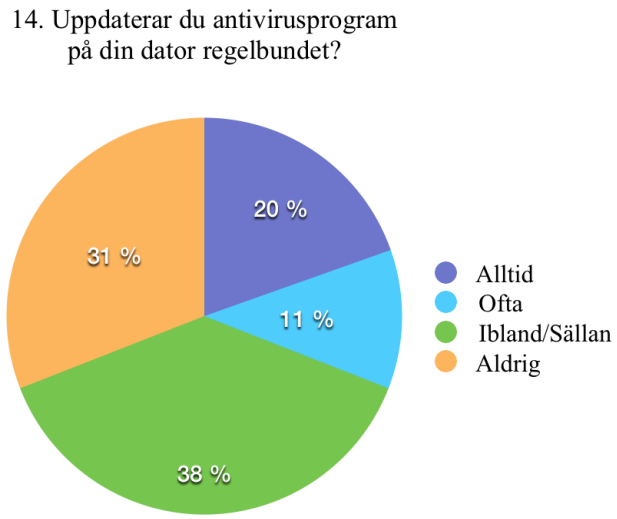
En problematik som uppstod gällande denna fråga var att majoriteten av respondenterna angav fler än en kunskapskälla till deras kunskap om nätbrott. Det hade varit önskvärt att de endast valt ett alternativ då det hade blivit enklare att framställa korrekt data i diagram, dock misstolkades frågan och majoriteten av respondenterna ringade in mer än ett svarsalternativ. För att kunna framställa ett diagram togs ett beslut om att inte utesluta något av svaren. Detta då det är av stor betydelse att få insikt i om vart individer får sin kunskap om nätbrott ifrån. Deltagarna fick välja mellan TV, radio, tidning, internet, vänner/familj samt alternativet att de inte har hört något. Totalt angav de 97 respondenterna 225 svar på fråga 13, vilket innebär att respondenterna i snitt angav två till tre svar. Därmed presenteras de 225 svaren i diagrammet nedan för att rent procentuellt få en överblick om vart individer fått kunskap om nätbrott ifrån.



Figur 13.

Fråga 14. *Uppdaterar du antivirusprogram på din dator regelbundet?*

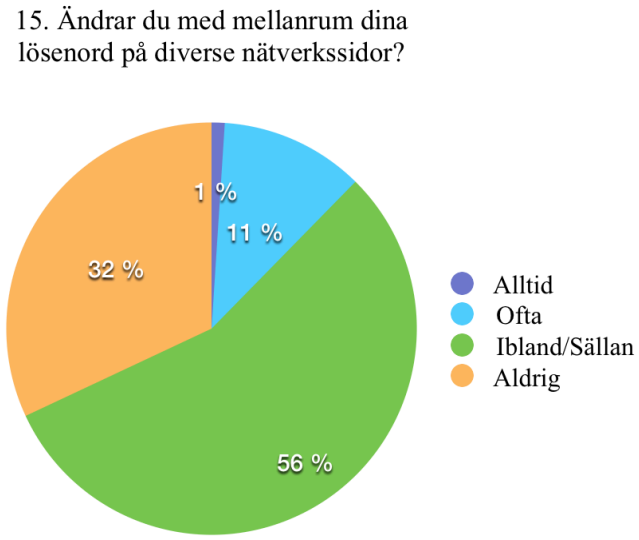
19 deltagare (20 procent) uppgav att de alltid uppdaterar sitt antivirusprogram på datorn regelbundet. Elva deltagare (elva procent) uppgav att de ofta uppdatera antivirusprogram på sin dator. 37 deltagare (38 procent) uppgav att de ibland/sällan uppdaterar sitt antivirusprogram och 30 deltagare (31 procent) uppgav att de aldrig uppdaterar antivirusprogram.



Figur 14.

Fråga 15. *Ändrar du med mellanrum dina lösenord på diverse nätverkssidor?*

En deltagare (en procent) uppgav att hen alltid ändrar lösenord med mellanrum på diverse nätverkssidor. Elva deltagare (elva procent) uppgav att de ofta ändrar lösenord med mellanrum på diverse nätverkssidor. 54 deltagare (56 procent) uppgav att de ibland/sällan ändrar lösenord och 31 deltagare (32 procent) uppgav att de aldrig ändrar lösenord.



Figur 15.

Fråga 16. *Gör du något mer för att skydda dig mot brott på nätet?*

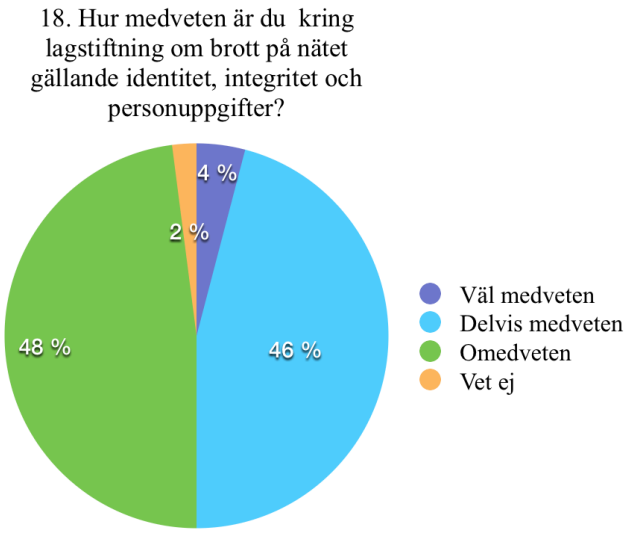
Likt fråga tio utfördes en kvalitativ innehållsanalys i ett sökande för att finna genomgående teman samt begrepp i svaren i både fråga 16 och 17. I den här frågan ombads respondenterna att uppge om de gör något mer aktivt för att skydda sig mot brott på nätet. Detta genom att besvara fråga med ett kvalitativt svar i form av skriven text. 43 deltagare uppgav olika beskrivningar gällande hur de skyddar sig mot nätbrott, medan 54 deltagare svarade att de ej gör något för att skydda sig mot denna typ av brott. Sex deltagare uppgav att de undviker konstiga sidor eller använder sig av säkra sidor. Nio deltagare uppgav att de använder sig av många olika lösenord eller att de använder sig av avancerade lösenord. Nio respondenter uppgav att de undviker att dela med sig av information om sig själva online, eller att de har privata konton. Två deltagare uppgav att de använder sig av antivirusprogram eller har en Mac och behöver därmed inte antivirusprogram. Elva deltagare uppgav att de är noga med vilka länkar de går in på och de undviker även att autospara diverse personuppgifter i from av bankuppgifter, telefonnummer eller adress. Resterande svar skilde sig åt och därmed presenteras de separat. En person angav att hen ej tillåter olika program som Javascript och att hen ofta rensar så kallade cookies från sin dator. En deltagare uppgav att hen har försäkring mot identitetsstöld online och en annan deltagare uppgav att hen använder sig av skatteverkets identitetsstöldsvarning. En annan deltagare uppgav att hen har flera mail inboxar för att sortera eventuella skräpmail och en annan deltagare uppgav att hen raderar konstiga mail. Slutligen uppgav en deltagare att hen läser sidors användarvillkor.

Fråga 17. *Hur trygg känner du dig på internet?*

I den här frågan uppgav 54 deltagare att de känner sig ganska trygga på internet, men beroende på vilken situation eller webbsida som de besöker kan det uppstå en viss oroskänsla. 14 deltagare uppgav att de känner sig trygga eller tillräckligt trygga för att använda internet, och de känner ingen oro. Fem deltagare uppgav att de känner sig inte helt trygga och bland dessa fem var det en deltagare som uppgav att hen är rädd för att hängas ut på internet. Fem deltagare uppgav att de känner sig otrygga eller rädda för att utsättas för nätbrott eller virus. En deltagare uppgav att hen ibland känner sig orolig vid bokning av varor eller tjänster internationellt. Tolv deltagare uppgav att de känner sig väldigt trygga och bland dessa tolv var det en person som angav att det aldrig känns som ett orosmoment. Två deltagare uppgav att de känner sig ganska trygga på sidor som de anser som seriösa, exempelvis Facebook. Bland dessa två var det dock en deltagare som erkände en viss osäkerhet gällande Facebook användande, och att hen ställde sig kritisk gällande sin tilltro till Facebook. Tre deltagare svarade att de känner sig ganska trygga men att de vid närmare eftertanke inser att risken att utsättas för nätbrott är relativt stor, och att de vill skaffa sig mer kunskap om ämnet. En sista deltagare uppgav att hen känner sig rätt trygg samt att hen sällan har konton på oseriösa hemsidor och anser att Facebook är trygg.

Fråga 18. *Hur medveten är du kring lagstiftning om brott på nätet gällande identitet, integritet och personuppgifter?*

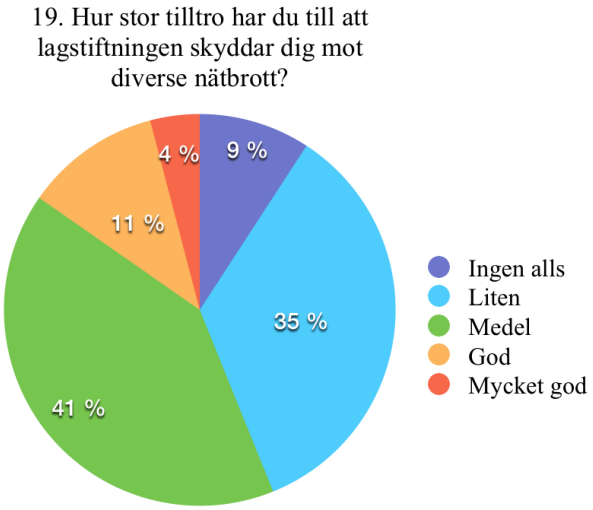
Fyra deltagare (fyra procent) uppgav att de är väl medvetna kring lagstiftningen om brott på nätet gällande identitet, integritet och personuppgifter. 45 deltagare (46 procent) uppgav att de är delvis medvetna om lagstiftningen kring denna typ av brott. 46 deltagare (48 procent) uppgav att de är omedvetna kring lagstiftningen och två deltagare (två procent) uppgav att de ej vet något om lagstiftningen gällande identitet, integritet och personuppgifter.



Figur 18.

Fråga 19. *Hur stor tilltro har du till att lagstiftningen skyddar dig mot diverse nätbrott?*

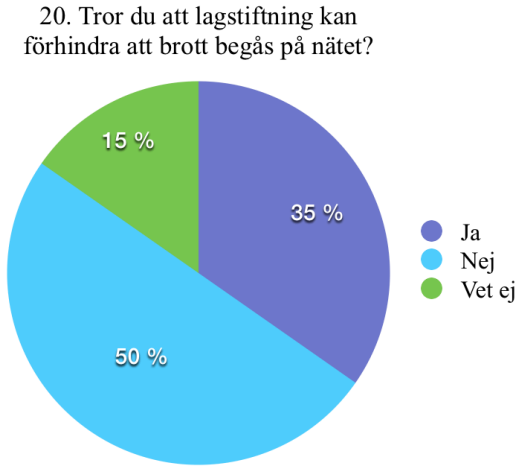
Nio deltagare (nio procent) uppgav att de inte har någon tilltro alls till att lagstiftningen kan skydda dem mot diverse nätbrott. 34 deltagare (35 procent) uppgav att de har en liten tilltro till lagstiftningens förmåga att skydda dem mot diverse nätbrott. 40 deltagare (41 procent) uppgav att de har medel tilltro till lagstiftningens skydd vid denna typ av brott. Tio deltagare (elva procent) uppgav att de har en god tilltro till lagstiftningen förmåga att skydda mot diverse nätbrott och fyra deltagare (fyra procent) uppgav att de har mycket god tilltro till lagstiftningen.



Figur 19.

Fråga 20. *Tror du att lagstiftning kan förhindra att brott begås på nätet?*

34 deltagare (35 procent) uppgav att de tror att lagstiftningen kan förhindra att brott begås på nätet. 48 deltagare (50 procent) uppgav att de inte tror på att lagstiftningen kan förhindra att brott begås på nätet och 15 deltagare (15 procent) gav ej ett svar vad de anser om lagstiftningens förmåga att förhindra nätbrott.



Figur 20.

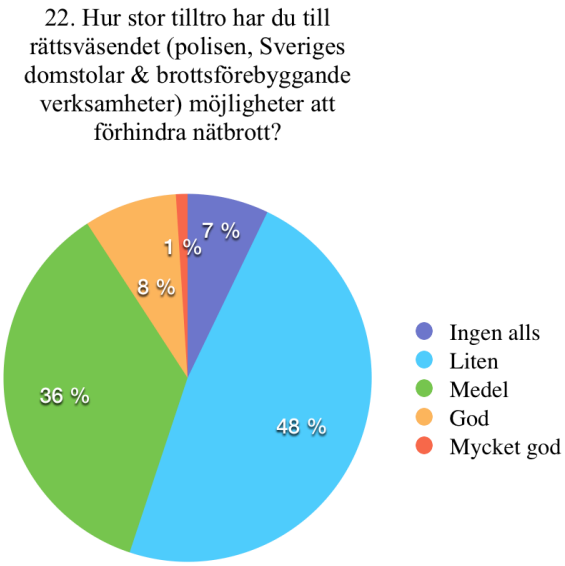
Fråga 21. *Om nej, vad beror det på?*

Denna fråga skulle enbart besvaras ifall respondenten svarade nej på fråga 20. 48 deltagare som svarat nej på fråga 20, besvarade även fråga 21. Det fanns även tre personer som fyllt i ja samt vet ej på fråga 20 som även besvarade fråga 21. Likt de resterande öppna frågorna gjordes en kvalitativ innehållsanalys av respondenternas svar. Sex deltagare uppgav att brott begås trots att lagstiftning existerar eftersom människor inte bryr sig om lagstiftningen och straffen är för dåliga. Sju deltagare uppgav att det är för lätt att vara anonym och att lagen därmed ej hjälper. Fem deltagare uppgav att lagen inte är tillräckligt stark och att den ej kan påverka eller stoppa individer som vill begå brott. Fyra deltagare uppgav att det är svårt att kontrollera vad som läggs ut på nätet och att det skulle krävas oerhörda resurser för att straffa folk. En av deltagarna menar bland annat att lagstiftningen kring vad som får och inte får publiceras skulle innebära en inskränkning av andras rättigheter. Nio deltagare hävdar att lagstiftningen alltid kommer ligga efter i utvecklingen och därmed kommer det alltid finnas kryphål i lagen som aldrig går att förhindra helt. Respondenterna nämnde även att fokus nog bör läggas på att försöka förhindra samt förebygga nätbrott så gott det går. En deltagare ansåg att polisresurserna är låga, snarare än att lagstiftningen brister, medan en annan deltagare menar att lagstiftningen varken

har kunskap eller resurser. En av deltagarna hävdar att lagstiftningen endast fungerar avskräckande, medan en annan deltagare anser att lagen enbart kan fungera som straff i efterhand. Två deltagare uppgav att det är för svårt att få tag på brottslingar, då de har större kunskap och de hittar snabbare sätt att komma undan, än vad rättsväsendet hinner med. De menar även att lagarna antagligen snabbt kommer att bli inaktiva då den högteknologiska utvecklingen går allt fortare framåt. En respondent svarade även att svensk lagstiftning saknar pondus gällande nätbrott och att den inte kommer kunna täcka brott som begås globalt på nätet. En deltagare tillade även att lagstiftning i regel är nationell men att internat är globalt, och det är där problematiken ligger gällande lagstiftning online. Fem deltagare uppgav att det är svårt att bestraffa brottslingar som begår nätbrott då de ofta är väldigt skickliga att dölja spår. En deltagare menade att hen inte anser att det sker mycket brott på nätet och att denna typ av brott därför ej prioriteras. En av deltagarna ansåg att lagstiftningen ej bryr sig och en annan deltagare skyllde på patriarkata strukturer. En deltagare uppgav att hen ej har förtroende för lagstiftning vad gäller nätmobbning då hen varit vittne till detta och menar att det händer allt för ofta.

Fråga 22. *Hur stor tilltro har du till rättsväsendet (polisen, Sveriges domstolar & brottsförebyggande verksamheter) möjligheter att förhindra nätbrott?*

Sju stycken deltagare (sju procent) uppgav att de inte har någon tilltro till rättsväsendet överhuvudtaget. 46 deltagare (48 procent) svarade att de hade en liten tilltro och 35 stycken (36 procent) svarade att deras tilltro till rättsväsendet kunde beskrivas som medel. Åtta respondenter (åtta procent) uppgav att de har en god tilltro till rättsväsendet och endast en person (en procent) uppgav att hens tilltro var mycket god.



Figur 22.

5. Analys och diskussion

I den kvantitativa undersökningen som genomfördes bland unga vuxna i Lund framgick det att alla deltagare i studien har ett konto på ett socialt nätverk, och att 98 procent använder sig av tjänsterna dagligen. Detta visar på att många idag använder sig av internet dagligen, och det är även något som går att se i Larssons artikel där han lyfter fram att 89 procent av Sveriges befolkning använder sig av internet (2014, s. 80–81). För att ytterligare undersöka unga vuxnas internetanvändande ställdes ett antal frågor om deras beteenden online. Det framgick att 48 procent aldrig läser webbsidors användarvillkor och att nio procent alltid sparar sina lösenord online och att 43 procent ofta gör det. Det går därmed att se att många unga vuxna utsätter sig själva för en del risker online. När personer ej läser webbsidors användarvillkor går de miste om information gällande lagring av personuppgifter och annan personlig data (*Facebook follies*, 2011). Vilket skulle kunna innebära att människor inte är medvetna om vart i cyberspace deras uppgifter hamnar och i vilket syfte de kan användas av andra. Det kan därmed ses som en tillverkad risk då användarna själva väljer att ej läsa användarvillkor och därmed utsätter sig själva för risktagande (Beck, 2000 s. 33, Newburn, 2013 s. 901–902). Det Beck menar med tillverkade risker är de risker människan själv skapar med sina handlingar och som kan förhindras beroende på hens handlingar (ibid.). Detta kan därmed kopplas till unga vuxnas val av handlingar som sker i cyberspace. En tillverkad risk online kan exempelvis vara att ange personliga uppgifter på exempelvis Facebook, då man eventuellt riskerar att ge en obehörig möjligheten att ta del av dessa uppgifter. Individer kan därmed minska risken att utsättas för denna typ av tillverkade risker genom att inte uppge sina uppgifter offentligt i cyberspace, och på så sätt undvika denna typ av risk. Ytterligare ett exempel som kan ses som en tillverkad risk online kan vara att autospara lösenord samt att besöka diverse opålitliga webbsidor. Detta är en risk som kan undvikas beroende på individens handlande då denne kan göra ett aktivt val att ej spara lösenord eller besöka diverse sidor. Sparar en person exempelvis lösenord eller besöker opålitliga sidor kan detta således leda till att personuppgifter läcks ut och sprids vidare ifall de hamnar i fel händer, vilket kan öka risken för att utsättas för nätbrott (Oweis, et al. 2014 s. 3). Att därmed ej spara lösenord på diverse nätverkssajter kan minska risken för att obehöriga får tillgång till personliga uppgifter.

95 procent av unga vuxna angav att de någon gång uppgett personliga uppgifter på nätet i form av namn, personnummer, bankuppgifter eller adress. En intressant aspekt som Cluley

lyfter fram ovan är att om en individ ej är beredd på att gå ut på en offentlig plats i den fysiska världen och ropa ut sina personuppgifter så borde hen ej ange de på internet (*Facebook follies,* 2011). Det kan därmed ses som anmärkningsvärt varför individer då väljer att ange personliga uppgifter på internet. Som det framgick av den kvantitativa undersökningen går det att argumentera för att en del unga vuxna har stor tillit till Facebook som de kallar för en pålitlig och seriös nätverkssajt. Cluley hävdar dock att Facebook idag är den främsta nätverkssidan för att begå nätbrott och få tag på individers personliga uppgifter och på så sätt kränka deras integritet (ibid.). Detta kan därmed innebära att unga vuxna inte är tillräckligt medvetna om de risker som finns i samband med sociala nätverkssajter som exempelvis Facebook.

Dock är människor idag tvungna att uppge personliga uppgifter i samband med dagliga aktiviteter som sker online. Detta då många nätverk och tjänster kräver att internetanvändaren uppger personliga uppgifter. Exempelvis kräver diverse banktjänster att individer måste uppge personuppgifter online för att komma åt sina konton (*Nordeas internetbank*, 2017). Även andra företag använder sig av onlinetjänster vid köp av tjänster samt varor då kunderna även här är tvungna att ange personuppgifter, bankuppgifter samt e-mailadress för att kunna genomföra ett köp. Detta skapar i sin tur en mängd risker för internetanvändarna som använder sig av diverse tjänster online, då det finns individer som besitter kunskaper om att utföra exempelvis dataintrång. Det blir därmed svårt att skydda sig mot de här typerna av nätbrott då dagens högteknologiska samhälle mer eller mindre är uppbyggt med hjälp av internettjänster. Detta i syfte för att framförallt underlätta dagliga uppgifter och aktiviteter för människor. Då 94 procent av respondenterna uppgav att de är medvetna om att nätverkssajter kan missbruka deras personliga uppgifter tyder detta på att unga vuxna är medvetna om de risker som finns. Trots detta väljer majoriteten att utsätta sig för de potentiella risker som finns med att uppge personliga uppgifter. Det blir här då intressant att lyfta fram Jung Kim och Hancocks teori om att människan besitter en optimistisk bias, då människan tror att chansen att något ska hända denne själv är relativt liten (2015, s. 214–215). Denna optimistiska bias kan möjligtvis bidra till att förklara varför en del unga vuxna utsätter sig för diverse risker som finns i samband med internetanvändande. Detta då det framgick av respondenterna i fråga sju att 33 procent är väl medvetna om de risker som finns medan 61 procent uppgav att de är delvis medvetna om riskerna online. Majoriteten av respondenterna (82 procent) angav även att de är medvetna om brottsligheten som sker online gällande personuppgifter samt integritet. Dock är endast 30 procent oroliga för att utsättas för diverse nätbrott och detta kan innebära att unga vuxna är medvetna om riskerna men de tror ej att de kommer hända dem själva. Detta visar ytterligare

på att unga vuxna är medvetna om risken att utsättas för brott på nätet, men att de ändå eventuellt värderar fördelar med internetanvändning högre än nackdelarna (2015, s. 214–215).

De respondenter som angav att de känner oro att utsättas för nätbrott ombads utveckla orsaken till denna oroskänsla. Det framgick dels att berättelser från andra som blivit utsatta för nätbrott påverkat respondenternas oroskänsla. Detta kan ha lett till att vissa respondenter blivit mer medvetna om att risken finns för att utsättas för nätbrott. 13 deltagare uppgav att de känner sig oroliga för att känsligt material som bankuppgifter skall hamna i fel händer och därmed även missbrukas. Tre deltagare uppgav även att de känner oro för att bli offer för identitetsstöld. Två deltagare uppgav att de inte har tillräckligt med kunskap om hur de skall skydda sig mot denna typ av brott på nätet. Anledningen till att en del av respondenterna kan uppleva en känsla av oro för att deras personliga uppgifter skall läcka ut kan bero på att det ej är önskvärt att bli offer för diverse nätbrott. Det kan därmed anses som att de här respondenterna besitter en viss kunskap och medvetenhet om diverse risker som finns men att de inte vet om hur de ska skydda sig. Respondenterna fick även ange vilken typ av nätbrott som de är mest oroliga att utsättas för och det visade sig att merparten var oroliga för att utsättas för identitetsstöld (26 procent), stöld av bankuppgifter (37 procent) samt dataintrång eller hacking (26 procent). Detta tyder på att majoriteten av unga vuxna i denna studie är mest oroliga för att deras personliga uppgifter skall hamna i fel händer.

Det ovan nämnda kan kopplas till Böhme och Moores studie där de redogör för individer som blivit exponerade för information om nätbrott eller hört berättelse från bekanta som blivit utsatta för nätbrott. De personer som fått mer kunskap om nätbrott uppgav att de känner en viss oro för att utsättas för denna typ av brott och använder därmed internet med större försiktighet (2012, s. 1). På samma sätt kan det antas att unga vuxna i den här studien som uppgav att de hört berättelser om nätbrott eller de som angett att de saknar kunskap upplever en större oroskänsla kring nätbrott.

Hälften av unga vuxna i denna studien uppgav att de har en liten kunskap eller ingen alls om hur de kan skydda sig mot diverse nätbrott. Detta är även något som Oksanena och Keipi lyfter fram när de pratar om att unga vuxna är mindre erfarna om de risker som internetanvändande innebär. De diskuterar även att unga vuxna är mer naiva i sitt beteende på internet och att de därför löper större risk för att utsättas för nätbrott (2013, s. 306–307). Detta visar tydligt på att det finns en bristande kunskap bland unga vuxna i denna studie. I studien framgick det även att majoriteten av deltagarna fått sin kunskap om nätbrott från internet samt bekanta. Cassim lyfter fram att behovet av ökad kunskap kring nätbrott är stort då många individers rättigheter kränks när de utsätts för diverse nätbrott (2015, s.71–72). Han menar även

att ansvaret ligger hos diverse organisationer samt internetleverantörer i att utbilda användarna om säker surfing eller erbjuda diverse säkerhetspaket (2015, s. 95–96). Andra sätt att minska risken för att utsättas för exempelvis dataintrång eller hacking kan vara att använda sig av antivirusprogram samt att regelbundet byta lösenord på sociala nätverkssajter. Dock tar majoriteten av respondenterna inte hänsyn till detta då enbart 31 procent uppdaterar sitt antivirusprogram ofta eller alltid. Dessutom är det endast en procent som alltid med mellanrum ändrar sina lösenord och elva procent som gör det ofta, vilket innebär att väldigt få tänker på att byta lösenord. På så sätt utsätter sig människor för ett onödigt risktagande som hade kunnat förhindras med hjälp av antivirusprogram eller ändring av lösenord. För att ytterligare undersöka ifall unga vuxna gör något mer aktivt för att skydda sig mot diverse nätbrott ombads respondenterna utveckla sina svar. Mindre än hälften uppgav att de aktivt skyddar sig mot nätbrott, detta genom att undvika opålitliga sidor, använda sig av olika och svåra lösenord, att undvika att uppge personlig information, att de använder antivirusprogram eller att de har en Mac dator. Andra uppgav att de undviker att autospara lösenord eller andra uppgifter, att de läser sidors användarvillkor, har olika mailboxar, rensar cookies från datorn eller har försäkring mot identitetsstöld. Detta tyder därmed på att det finns vissa individer som är medvetna om riskerna och som försöker skydda sig mot diverse nätbrott i den mån det går. Även trygghetskänslan påverkas beroende på hur stor kunskap respondenten har om hur hen skall skydda sig. De som har tillit till exempelvis säkra sidor enligt dem själva uppgav att de känner sig trygga. Dock känner sig vissa oroliga vad gäller oseriösa sidor samt vid onlineköp av diverse tjänster och varor. De blir här även intressant att lyfta fram att tre respondenter känner sig trygga på den sociala nätverkssajten Facebook. Detta visar på att det finns individer som saknar både kunskap och medvetenhet om hur sociala nätverkssajter kan lagra användarnas data och att personuppgifter på så sätt kan missbrukas av obehöriga. Det är något som framför allt lyfts fram i dokumentären *Facebook follies* där diverse experter uttalar sig om hur Facebook kan användas som en källa för att få tag på människors personuppgifter (2011). Medvetenhet och kunskap kan därmed argumenteras för att vara av stor vikt för att undvika eller försöka minska riskerna online.

För att få insikt i hur medvetna unga vuxna är kring lagstiftning om brott på nätet gällande identitet, integritet och personuppgifter undersöktes detta i fråga 18. 48 procent uppgav att de är omedvetna om lagstiftningens existens gällande brott på nätet, 46 procent angav att de är delvis medvetna och att endast fyra procent är väl medvetna om lagstiftningen. Detta tyder på att det finns en bristande medvetenhet bland unga vuxna om lagstiftningen, vilket kan anses problematiskt då lagen har som uppgift att skydda samt ge en känsla av trygghet.

Dock verkar majoriteten, 56 procent av respondenterna, ha en medel eller god tilltro till att lagstiftningen kan skydda dem mot diverse nätbrott. Dock uppger 44 procent att de har liten eller ingen alls tilltro till lagstiftningen. Detta kan kopplas till Enarsson som hävdar att det kan uppstå en övertro till lagstiftningens möjligheter att reglera brott på nätet. Detta skulle kunna innebära att de 56 procent som tror att lagstiftningen kan skydda dem mot nätbrott har denna övertro som Enarsson lyfter fram i sin artikel (2015). Det blir dock intressant när respondenterna ombads besvara frågan gällande ifall de tror att lagstiftning kan förhindra att brott begås på nätet. Detta eftersom endast 35 procent uppgav att de tror att lagstiftningen kan förhindra att brott begås på nätet. Därmed går det att ifrågasätta hur 56 procent kan ange att de känner tilltro till lagen men samtidigt är det endast 35 procent som anger att de tror att lagstiftningen kan förhindra nätbrott.

I fråga 21 ombads respondenterna som i fråga 20 uppgett att de ej tror att lagstiftning kan förhindra brott att utveckla sina svar. Det framgick av svaren att unga vuxna ej tror att lagstiftningen kan påverka eller stoppa individer från att begå brott, detta då det är så enkelt att vara anonym och det är globalt. Respondenterna angav även att straffen är för låga, att det saknas resurser och kunskap inom rättsväsendet och att det är svårt att bestämma vad som får publiceras och inte. Dock påstod majoriteten att lagstiftningen aldrig kommer att hinna utvecklas och stiftas i samma takt som internets framväxt och att lagen alltid kommer att ligga efter samt bli ineffektiv. Respondenternas svar speglas även i Enarssons artikel där hon lyfter fram att stiftande av nya lagar inte nödvändigtvis är den ultimata lösningen. Hon nämner även att det kan vara svårt för lagstiftningen att anpassas till den tekniska utvecklingen som internet innebär (2015).

Det framgår även i respondenternas svar att det inte endast är lagstiftningen som har en relativt liten tilltro utan att även rättsväsendets förtroende sviktar. Endast åtta procent uppgav att de har en god tilltro medan 48 procent uppgav att det har en liten tilltro till rättsväsendet. När ett litet antal individer har tilltro till rättsväsendets förmåga att bekämpa nätbrott kan detta enligt Enarsson resultera i att det blir ytterligare svårare att utreda samt bekämpa denna typ av brott. Detta kan bero på att personer som exempelvis utsätts för nätbrott väljer att ej anmäla detta då de inte tror att rättsväsendet kan hjälpa dem (ibid.).

En diskussion som uppstår i samband med internet och de risker som förekommer online är svårigheten att utföra reglering med hjälp av lag i detta virtuella rum. Detta då det uppkommer svårigheter i att fastställa tydliga gränser i det globala cyberspace och med den anonymitet som råder i detta rum (Lino, 2015 s. 87). De utmaningar som internet medfört för lagstiftarna har skapat en diskussion kring huruvida internet skall styras och av vem

(Mathiason, 2009 s. xiv). Det finns de som hävdar att självreglering av internet skulle kunna vara en möjlig lösning för problematiken kring regleringen av internet. Cogburn lyfter bland annat fram internet governance som innebär en slags styrning av internet. Cogburn med kollegor beskriver denna internetstyrning som en utformning och tillämpning av kollektiva policies för det globala internetsamhället (Cogburn, et al. 2005 s. 12). Detta kan förklaras som att det är önskvärt att skapa gemensamma policies för hur internet skall styras bland användarna. Det kan därmed innebära att sociala normer bör internaliseras i samhället, och även i onlinesamhället om hur internet skall användas av internetanvändarna. Även Johnson och Post hävdar att cyberspace bör regleras av själva internetanvändarna då det är de som använder sig av internet (Lino, 2015 s. 92).

Det är dock här frågan uppstår om det ens är möjligt att utföra en självreglering och hur internetanvändarna skall kunna reglera internet om de ej har kunskap om hur detta bör göras. Det kan även anses väldigt problematiskt att komma fram till allmänt accepterade normer på internet då individer använder internet för så många olika områden. Det står dock klart för de flesta forskarna som nämnts ovan att lagstiftning kring diverse beteende online är svårt att styra i cyberspace. Det benämns även av respondenterna i enkätstudien att de anser att lagen ej kan förhindra brott på nätet. Detta då cyberspace används globalt och att många användare är anonyma och det ej går att tillämpa lagen på en viss person för ett specifikt brott. Internet utvecklas dessutom ständigt och därmed kan nya risker uppstå vilket blir svårt att reglera. Vi som människor kan idag inte säga hur internet kommer att utvecklas samt vilka potentiella risker som kommer att uppstå tack vare detta. Det blir därmed ännu svårare att förutspå dessa nya risker. Det kan även argumenteras för att det finns lagstiftning som kan tillämpas för de brott som sker på nätet, som exempelvis identitetsstöld, men att det är svårare att finna den skyldige personen på grund av anonymitet. Lagen kan därmed i mindre utsträckning tillämpas som sanktionsmedel mot den skyldige i de fall brottet har begåtts online. Detta tyder delvis på att dagens lagstiftning kan anses bristande, eftersom de traditionella lagarna inte är tillräckligt anpassade till de brott som sker i det virtuella rummet.

Det kommer därmed bli svårt att reglera risker i samhället med hjälp av rätten. Det är snarare en fråga om huruvida rätten kan samverka med sociala normer för att åstadkomma en reglering av internet och människors beteende online. Sociala normer kan anses vara “friare” samt gemensamt bestämda, vilket kan leda till att fler väljer att acceptera dem. De får heller ej den strikta och hårda ton som regler få när de stiftas av makthavarna. Normer kan även påstås ha en enklare spridningsförmåga då de ofta överförs från person till person, eller att de uppkommer i grupper och kan därmed anses lättare att få kunskap om samt att efterleva (Hydén,

2002 s. 96). Lagen kan anses som ett påtryckande verktyg för att reglering skall ske i samhället, då social ordning är av stor vikt för att ett samhälle skall fungera friktionsfritt. På så sätt krävs det sociala normer som influeras av lagen men som gemensamt beslutas av internetanvändarna. Då svensk lag aldrig kommer att kunna styra de globala riskerna som finns på internet är det individers egna beteende och risktagande som måste regleras och styras med hjälp av sociala normer, för att undvika brottslighet på nätet i den mån det går. Det är även av stor betydelse att öka medvetenheten samt kunskapen bland människor för att på så sätt undvika samt minska risker att utsättas för nätbrott. Risker är något som alltid kommer finnas, det går dock att bli bättre på att minska dessa risker. Rätten och sociala normer bör därmed samverka för att internalisera ett allmänt accepterat beteende online. Det är dock viktigt att vara medveten om att det alltid kommer finnas de som vill bryta mot normer och regler, vilket inte går att undvika helt.

6. Slutsatser

I den här studien ställdes frågan vilken kunskap och medvetenhet unga vuxna har om de risker som finns på nätet gällande integritet och personuppgifter. Det eftersöktes även svar på hur detta kan påverka deras internetanvändande. Svaren som angavs i fråga sex tyder på att unga vuxna verkar ha en hög medvetenhet (94 procent) om att sociala medier och andra internetsidor kan lagra och missbruka känsligt material. Även svaren i fråga sju tyder på att unga vuxna är medvetna om de risker som uppstår i samband med internetanvändande. Detta då 94 procent angav att de är väl eller delvis medvetna om riskerna online. Många angav även att de är medvetna (82 procent) om brottslighet som sker online, vilket kan antas innebära att de även är medvetna om att det finns en risk att utsättas för nätbrott. Detta kan därmed tolkas som att unga vuxna är väl medvetna om de risker som finns i samband med internetanvändande. Resultaten skiljer sig dock när frågan ställs om vilken kunskap unga vuxna har om hur de kan skydda sig mot nätbrott. Hälften av respondenterna angav (50 procent) att de har en liten eller ingen kunskap alls om hur de kan skydda sig. I detta fall kan kunskapen anses bristande bland unga vuxna. Fråga 14, 15 och 16 berör hur unga vuxna använder sina kunskaper för att skydda sig mot nätbrott. 31 procent uppgav att de alltid eller ofta uppdaterar antivirusprogram på sina datorer, medan 69 procent gör det sällan eller aldrig. Det går därmed att ställa frågan ifall detta beror på en okunskap om hur man kan skydda sig mot exempelvis virus eller om det beror på en lathet att ej uppdatera och skydda sig. Även när det gäller att ändra lösenord med mellanrum för att på så sätt skydda sig mot nätbrott, angav 88 procent att de sällan eller aldrig ändrar

lösenord. Det går även här att diskutera ifall unga vuxna besitter en okunskap om diverse sätt att skydda sig mot nätbrott, eller om det beror på andra orsaker. 43 av 97 deltagare besvarade fråga 16 där de beskrev mer utförligt vad de gör för att aktivt skydda sig mot nätbrott. Det kan antas att de här respondenterna besitter högre kunskap samt medvetenhet om diverse åtgärder för att skydda sig mot risker online.

För att därmed svara på den första frågeställningen verkar det som att medvetenhet bland unga vuxna är hög, men att kunskapen om hur de skall skydda sig mot risker online är relativt låg. Det eftersöktes även svar på hur detta kan påverka deras internetanvändande. Det går därmed att se att beroende på vilken medvetenhet samt kunskap de besitter så beter sig individer annorlunda på internet och det skiljer sig från individ till individ.

Den andra frågeställningen som berörs i studien är vilken attityd unga vuxna har till lagstiftningen gällande nätbrott samt rättsväsendets möjligheter att påverka denna typ av brott. Resultatet i studien visade bland annat att nästan hälften (48 procent) av respondenterna inte är medvetna kring lagstiftningen gällande identitet, integritet och personuppgifter. Trots detta uppger 56 procent av respondenterna att de har medel, god eller mycket god tilltro till att lagstiftningen kan skydda dem mot diverse nätbrott. Dock går det att ifrågasätta respondenternas tilltro till lagstiftningen då endast 35 procent uppger i följande fråga att de tror att lagen kan förhindra att brott begås på nätet. För att ytterligare undersöka unga vuxnas tilltro till rättsväsendet ställdes fråga 22. Här uppgav 55 procent av respondenterna att de har liten eller ingen tilltro alls till att rättsväsendet kan förhindra brott på nätet. Det går därmed att besvara den andra frågeställningen i den här studien med att unga vuxna har en relativt negativ attityd till lagen och rättsväsendets möjlighet att påverka och förhindra nätbrott. Framför allt då de anser att lagen har begränsade möjligheter i detta område och att rättsväsendet ej har de resurser eller kunskap som krävs.

Slutligen har den sista frågeställningen delvis berörts ovan under analys och diskussionsdelen. För att ytterligare besvara den sista frågeställning kring hur rätten och sociala normer kan samverka för att minska risken för nätbrott och öka medvetenheten lyfts följande förslag fram. Då rätten har makten att styra och påverka människors beteende och handlingar skulle lagstiftarna kunna införa obligatorisk utbildning i exempelvis skolor. Detta för att öka medvetenheten och kunskapen bland unga om de risker som finns online och för att främja ett säkert internetanvändande. Då lagen ej har möjlighet att ta bort risker som människor utsätts för på nätet hade det varit optimalt att införa lagstiftning som påverkar människors beteende online med hjälp av kunskap och utbildning. På så sätt kan människor få en förståelse om risker och säkert internetanvändande, sprida detta vidare till andra och på så sätt internalisera

beteendemönster online, med andra ord normer. Skulle en utbildning nå ut till större grupper i form av skolklasser eller arbetsplatser hade detta eventuellt lett till att människor får en gemensam uppfattning som blir allmänt accepterad gällande risker online.

Det är dock viktigt att vara medveten om att detta förslag kan vara svårt att genomdriva då det krävs en stor mängd resurser, tid, kapital och samarbete mellan diverse organisationer, men även nationer och stater. Det går därmed att ställa frågan om det ens är möjligt, det hade dock varit önskvärt ifall det varit genomförbart, då rätten samt sociala normer kunnat samverka på ett effektivt sätt. Detta förslag hade därmed eventuellt kunnat minska risken att utsättas för nätbrott och öka medvetenheten kring risker online.

6.1 Avslutande kommentar

Slutligen har resultatet i denna studie visat på att unga vuxnas medvetenhet är hög men att kunskapen var relativt låg gällande hur de skall skydda sig mot nätbrott och på så sätt minska risken att drabbas. Dessvärre är de risker på internet större än vad en del tror, framför allt då brottslingar kan vara anonyma och då dataintrång sker utan större tecken på offrets dator. Resultaten visade även på unga vuxnas bristande kunskap kring lagstiftningen online gällande identitet, integritet och personliga uppgifter. Det kan även anses problematiskt då individer som utsätts för diverse nätbrott kanske går miste om vilka rättigheter de har och hur lagen kan skydda dem. Vad studiens resultat dock visar på är att lagens möjligheter begränsas gällande nätbrott då det är svårt att styra anonyma användare som dessutom kan befinna sig på andra sidan jorden. Lagens möjlighet att täcka brott som begås online försvåras och skapar därmed en global problematik. När då rätten och övriga rättsväsendet även saknar kompetens och kunskap om hur denna typ av brott skall förhindras riskerar rättsväsendet att förlora tillit och förtroende hos medborgarna. Dock presenteras det i denna studie att tilliten och förtroendet bland unga vuxna är relativt låg för rättsväsendets möjligheter att påverka.

Förhoppningen med denna studie har därmed varit att öka medvetenheten kring risker som finns online gällande nätbrott. Detta då det är ett relativt nytt fenomen som många människor saknar kunskap om. Det kan dock anses ha nått ut till 97 stycken unga vuxna som befann sig på Lunds universitets campusområden under studiens genomförande. Detta då vi som forskare kunde höra vid insamlingen av enkäterna hur konversationer och diskussioner uppstod kring ämnet. Vi anser därmed att studien har lyft upp ämnet kring risker på nätet gällande nätbrott och vi lämnar nu över till framtida forskning för att ytterligare öka

medvetenheten och kunskapen kring risker online och hur människors beteende bör regleras i cyberspace.

7. Referenser

7.1 Vetenskapliga artiklar

Böhme, R. Moore, T (2012). ”How do consumers react to cybercrime?”. *Ecrime Researchers Summit, Ecrime Researchers Summit (Ecrime)*.

Cassim, F (2015) ”Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves”, *Potchefstroom Electronic Law Journal*, 2, p. 68.

Cogburn, D, Mueller, M, McKnight, L, Klein, H, & Mathiason, J (2005). ”The U.S. role in global internet governance”, *IEEE Communications Magazine*, 43, 12, pp. 12-14.

Daharaskar, R.V, Nirkhi, S.M, Thakre, V.M. (2012). ”Analysis of online messages for identity tracing in cybercrime investigation”. *Proceedings Title: 2012 International Conference On Cyber Security, Cyber Warfare And Digital Forensic (Cybersec), Cyber Security, Cyber Warfare And Digital Forensic (Cybersec)*.

Dahlstrand, K, Wigerfelt, B & Wigerfelt, A (2015). ”ONLINE HATE CRIME – SOCIAL NORMS AND THE LEGAL SYSTEM”, *Quaestio Iuris*, 3, p. 1859, SwePub.

De Vey Mestdagh, C, & Rijgersberg, R (2010). ”NTERNET GOVERNANCE AND GLOBAL SELF REGULATION: Theoretical and empirical building blocks for a general theory of self regulation”, *Legisprudence: International Journal For The Study Of Legislation*, 4, 3, pp. 385–404.

Drezner, D. W. (2004), ”The Global Governance of the Internet: Bringing the State Back In. Political Science Quarterly”, 119: 477–498.

Eskola, M (2012). ”From Risk Society to Network Society: Preventing Cybercrimes in the 21st Century”, *Journal Of Applied Security Research*, 7, 1, pp. 122–150.

Inouye, J (2014), ”Risk Perception:Theories, Strategies, And Next Steps”. *National safety council*. Campbell Institute.

Kim, J, & Hancock, J (2015) ”Optimistic Bias and Facebook Use: Self-Other Discrepancies About Potential Risks and Benefits of Facebook Use, Cyberpsychology, Behavior & Social Networking” 18, 4, pp. 214-220, Business Source Complete.

Kokswijk, J (2010). ”Social Control in Online Society--Advantages of Self-Regulation on the Internet”, *International Conference On Cyberworlds (CW)*, p. 239, Complementary Index, EBSCO*host*, viewed 5 June 2017.

Larsson, S. (2014). ”Digitaliseringens Rättssociologi. Om mätbarhetens behov av teori och den digitala arkitekturens normativa relevans”. *Retfeard: Nordisk Juridisk Tidsskrift*, 2, p. 77.

Lino, S (2015). ”Cyberspace regulation: cesurist and traditionalists”, *Janus.Net, Vol 6, Iss 1, Pp 86–99*, 1, p. 86.

MacDonald, M, & Lang, A (2014). ”Applying Risk Society Theory to findings of a scoping review on caregiver safety”, *Health & Social Care In The Community*, 22, 2, pp. 124–133.

Oksanen, A, & Keipi, T (2013). ”Young people as victims of crime on the internet: A population-based study in Finland”, *Vulnerable Children & Youth Studies*, 8, 4, pp. 298–309.

Oweis, N.E, Owais, S.S, Alrababa, M.A, Alansari, M, Oweis, W.G. (2014). ”A survey of Internet security risk over social networks”. *6Th International Conference On Computer Science And Information Technology (CSIT)*.

Palfrey, J (2010), ”Four Phases of Internet Regulation”, Social Research, 3, p. 981.

Putnik, N, & Bošković, M (2015) ”The Impact of Media on Students' Perception of the Security Risks Associated With Internet Social Networking - A Case Study”, *Croatian Journal Educational / Hrvatski Casopis Za Odgoj I Obrazovanje*, 17, 2, pp. 569–583.

Saridakis, G, Benson, V, Ezingeard, J, & Tennakoon, H (2016). ”Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users”, *Technological Forecasting & Social Change*, 102, pp. 320–330.

Svensson, M, Dahlstrand, K (2014). ”Nätkränkningar: en studie av svenska ungdomars normer och beteenden”, SwePub.

Wall, D.S (2013). ”Policing identity crimes”, *Policing & Society*, 23, 4, pp. 437–460.

7.2 Litteratur

Andersen, H & Kaspersen, L B. (red.) (2007). *Klassisk och modern samhällsteori*. 3., [utvidgade och rev.] uppl. Lund: Studentlitteratur.

Beck, U (2000). *Risksamhället: på väg mot en annan modernitet*. Göteborg: Daidalos.

Bryman, A (2008). *Samhällsvetenskapliga metoder*. 2., [rev.] uppl. Malmö: Liber.

Denscombe, M (2009). *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna*. 2. uppl. Lund: Studentlitteratur.

Hydén, H (2002). *Normvetenskap*. Lund: Sociologiska institutionen.

Mathiason, J (2009). *Internet Governance: The New Frontier Of Global Institutions*. London; New York: Routledge

Mathiesen, T (2010). *Rätten i samhället: [en introduktion till rättssociologin]*. Lund: Studentlitteratur

Newburn, T (2013). *Criminology*. 2nd ed. London: Routledge

7.3 Internetkällor

Andersson, F (2015). ”Nätkränkningar - få anmälningar leder till åtal”. Brottsförebyggande rådet. https://www.bra.se/nytt-fran-bra/arkiv/press/2015-02-02-natkrankningar---fa-anmalningar-leder-till-atal.html
Hämtad: 2017-06-05

Dina rättigheter enligt personuppgiftslagen
http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/dina-rattigheter/
Hämtad: 2017-05-15

Enarsson, T (2015). *Det finns risk för en övertro på lagstiftning när det gäller näthat*. Dagens juridik.
http://www.dagensjuridik.se/2015/02/det-finns-risk-en-overtro-pa-lagstiftning-nar-det-galler-nathat
Hämtad: 2017-05-15

IT-relaterade brott - Polisens arbete
https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/
Hämtad: 2017-05-16

Nationalencyklopedin, identitet
http://www.ne.se/uppslagsverk/encyklopedi/lång/identitet
Hämtad: 2017-05-15

Nordeas internetbank
https://internetbanken.privat.nordea.se/nsp/login
Hämtad: 2017-05-17

Personuppgifter i sociala medier
http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sociala-medier/
Hämtad: 2017-05-15

Publicering på internet
http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/publicering-pa-internet/
Hämtad: 2017-05-15

7.4 Dokumentär

Facebook förstörde mitt liv (2011). Tv4play. Amerikansk dokumentär med originaltitel ”Facebook Follies” (2011).

https://www.tv4play.se/program/facebook-f%C3%B6rst%C3%B6rde-mitt-liv?video_id=2373717

Hämtad: 2017-04-20

7.5 Offentliga publikationer

SFS 2014:302. Dataintrång. *Brottsbalken*. Stockholm: Justitiedepartementet.

SFS 1986:123. Datorbedrägeri. *Brottsbalken*. Stockholm: Justitiedepartementet.

SFS 1998:204. *Personuppgiftslagen*. Stockholm: Justitiedepartementet.

8. Bilagor

8.1 Enkät

LUNDS
UNIVERSITET

Enkät om medvetenhet att utsättas för brott på nätet och de risker som finns gällande identitet, integritet och personuppgifter

Din uppgift är att på nästa sida svara på en enkätundersökning gällande brott på nätet. Medverkan tar ca 5 minuter och du är helt anonym. Läs all information noga och svara uppriktigt på alla frågor.

Tack för din medverkan!

1. **Har du ett konto på något socialt nätverk online?**

   Ja Nej Vet ej

2. **Hur ofta använder du sociala nätverk online?**

   Aldrig

   Ibland

   1 gång i veckan

   2-3 gånger i veckan

   Dagligen

3. **Läser du exempelvis webbsidors användarvillkor?**

   Alltid Ofta Ibland/sällan Aldrig

4. **Brukar du spara dina lösenord och andra uppgifter vid inloggning på diverse sidor?**

   Alltid Ofta Ibland/sällan Aldrig

5. **Har du någon gång angett personliga uppgifter online som namn, personnummer, bankuppgifter eller adress?**

   Ja Nej Vet ej

6. **Tror du att internet och sociala nätverkssajter kan lagra och missbruka känsligt material gällande din integritet och personuppgifter?**

   Ja Nej Vet ej

7. **Hur medveten är du om olika risker med att använda internet, e-postkonton**

och sociala nätverkssajter?

Väl medveten **Delvis medveten** **Omedveten** **Vet ej**

8. Är du medveten om brottslighet som sker online gällande personuppgifter och integritet?

Ja **Nej** **Vet ej**

9. Känner du dig orolig att utsättas för brott på nätet gällande personuppgifter och integritet?

Ja **Nej** **Vet ej**

10. Om ja, vad orsakar denna oro?

Svar:_____

_____

_____

11. Vilken typ av nätbrott är du mest orolig att utsättas för?
(Fyll i max 2 svarsalternativ)

Identitetsstöld

Stöld av bankuppgifter

Hacking/Dataintrång

Näthat/Mobbning

Sexuella trakasserier

12. Har du kunskap om hur du kan skydda dig mot diverse nätbrott?

Inte alls

Liten

Medel

God

Mycket god

13. Vart eller vem har du fått kunskap ifrån om nätbrott?

Tv

Radio

Tidning

Internet

Från vänner, familj eller kollegor

Har inte hört något om nätbrott

14. Uppdaterar du antivirusprogram på din dator regelbundet?

Alltid **Ofta** **Ibland/sällan** **Aldrig**

15. Ändrar du med mellanrum dina lösenord på diverse nätverkssidor?

Alltid **Ofta** **Ibland/sällan** **Aldrig**

16. Gör du något mer för att skydda dig mot brott på nätet?

Svar: _____

_____

_____

17. Hur trygg känner du dig på internet?

Svar: _____

_____

_____

18. Hur medveten är du kring lagstiftning om brott på nätet gällande identitet, integritet och personuppgifter?

Väl medveten **Delvis medveten** **Omedveten** **Vet ej**

19. Hur stor tilltro har du till att lagstiftningen skyddar dig mot diverse nätbrott?

Ingen alls

Liten

Medel

God

Mycket god

20. Tror du att lagstiftning kan förhindra att brott begås på nätet?

Ja **Nej** **Vet ej**

21. Om nej, vad beror det på?

Svar:_____

_____

_____

22. Hur stor tilltro har du till rättsväsendet (polisen, Sveriges domstolar

& brottsförebyggande verksamheter) möjligheter att förhindra nätbrott?

Ingen alls

Liten

Medel

God

Mycket god

<u>Kön:</u> **Man** **Kvinna** **Annat**

<u>Ålder:</u> **Yngre än 20** **20-25** **25-30** **30+**