HØGSKULEN I VOLDA

| Boks 500 | 6101 Volda | Norway | T: 70 07 50 00 | F: 70 07 50 51 |
| E: postmottak@hivolda.no | www.hivolda.no |

Masteroppgave i Dokumentar og journalistikk

Journalister og dataangrep

Studiepoeng 45

Morten Åsland

05/2014.

Sammendrag

Denne oppgavens formål er å undersøke om norske journalister står ovenfor nye utfordringer i en verden hvor man legger fra seg store mengder digitale spor. Er det slik at journalister kan være mulige ofre, for et dataangrep hvor kriminelle aktører er på kildejakt? Jeg har intervjuet fem norske journalister med lang erfaring innenfor en rekke medier. Flere av dem har mistanke om at de er utsatt for dataangrep uten at dette er dokumentert. Oppgaven er utformet som et casestudie, og jeg har gjort kvalitative dybdeintervjuer med alle informantene.

Den digitale trusselen må ses på som en følge av teknologisamfunnet vi lever i, og ingenting tyder på at journalister er mindre utsatt enn andre samfunnsborgere. Funnene viser høyst sannsynlig at dataangrep har funnet sted, og samtidig at mange journalister begynner å ta viktige forholdsregler for å sikre informasjonen sin. Det er enda langt å gå i forhold til digitalt kildevern, men med Wikileaks-avsløringene til blant annet engelske *The Guardian* og amerikanske *New York Times* har mange blitt mer oppmerksomme på hvilket overvåkingssamfunn vi lever i. Informantene tror at dette kun er starten på et overvåkingssamfunn hvor man må ta nye hensyn for å opprettholde det hellige kildevernet.

Forord

Det har vært både spennende og lærerikt å jobbe med masteroppgaven. Temaet har det blitt gjort lite forskning på tidligere, noe som har ført til at utfordringene har stått i kø. Jeg håper derfor å kunne bidra med interessante perspektiver om en mediebransje som står ovenfor nye digitale utfordringer sammen med resten av samfunnet. Det er med stor takknemlighet at informantene jeg har intervjuet ønsket å dele sine historier om datakriminalitet.

Jeg ønsker å rette en takk til min veileder Pål Aam for mange gode samtaler og råd underveis i arbeidet med masteroppgaven. Han har alltid stilt opp når jeg har ønsket veiledning, og kommet med mange gode innspill på hva jeg burde fokusere på.

Innholdsfortegnelse

Kapittel 1: Problemstilling og kontekst

Teori og bakgrunn

Vi lever i en tid hvor det meste av teknologi vi benytter til kommunikasjon er tilkoblet Internett. For mange vil det være utenkelig at en PC, nettbrett eller mobiltelefon ikke kan brukes til å kommunisere med andre mennesker. Verden har kommet mye nærmere stuen, og man kan kontaktes når som helst fra hvor som helst. Det som før var langt borte er nå bare noen tastetrykk unna, og distansen mellom landene er visket ut. Vi kan spores nesten overalt hvor vi beveger oss ved hjelp av elektroniske verktøy. Enten vi bruker mobiltelefon, Internett, blir filmet av overvåkningskameraer eller betaler med bankkort i butikken er det mulig å finne ut hvor vi har vært. Det er meget vanskelig å unngå å legge fra seg elektroniske spor, og det er alltid noen der ute som kan *følge med oss*.

Dersom man gjør et enkelt Google-søk på seg selv ser man hvor mye informasjon som ligger tilgjengelig for allmennheten. Er det en slik verden vi ønsker å leve i, og hva kan dette bety for journalistikken? Dette er bare overflaten av Internett, og har man gode digitale ferdigheter kan man finne informasjon som tar pusten fra de fleste av oss. Kriminelle miljøer utvikler nye metoder i det elektroniske rommet til kriminalitet (Internett), og de starter ofte med å samle sammen så mye informasjon om deg som overhodet mulig. Man har også muligheten til å kjøpe skreddersydde verktøy og kompetanse på Internett for å få utført kriminelle elektroniske handlinger.

> Datakriminalitet blir mer organisert og internasjonal, og vi ser tydeligere vinningsmotiv. I tillegg kan vi se at det i stadig sterkere grad blir tatt i bruk ny teknologi når tradisjonell kriminalitet begås. Eksplosjonen for Internett-brukere gir et marked for å utvikle programmer og utstyr som kan spionere og rapportere om brukeraktiviteter der man enkelt kan tappe passord og brukeridentitet sier sjefen i datakrimavdelingen i Kripos Rune Fløisbonn (Bye & Sjue, 2008, s. 332).

Dagens overvåkning er av en slik natur at ingen kan unngå den. Den angår oss alle, og jo flere spor vi legger i fra oss, jo enklere er det for overvåkeren å kontrollere hva vi gjør. Det at noen blir overvåket har skjedd før og er derfor ikke noe nytt. Hva er det som står

på spill for journalister som blir overvåket av myndigheter, politi, hemmelige tjenester eller private interesser?

Gravejournalister jobber med saker av stor samfunnsmessig interesse hvor kildene noen ganger må holdes anonyme. De siste årene har dataangrepene økt mot journalister og medier verden over, og kriminelle hackere tilbyr en billig måte å motarbeide eller sabotere pressen på. Sporene vi legger igjen trenger i seg selv ikke å være interessante. Det er først når man knytter sammen all informasjonen om personen som finnes på Internett at den kan brukes eller misbrukes. Kriminelle nettverk kan samordne informasjonen om deg i databaser, og organisere materialet på en slik måte at de sitter med en kunnskap som for noen år tilbake var utenkelig. Vi som er brukere av alle disse mediene er klar over faren om at det er noen som kan følge med oss. De fleste journalister er ikke klar over hvor store konsekvenser den digitale revolusjonen kan få for oss både positivt og negativt (Bye & Sjue, 2008, s. 51).

> Nettet har vokst raskere enn noe annet massemedium i historien: Ved utgangen av mars 2011 var det nesten 2,1 milliarder mennesker som brukte internett. Bare i 2009 ble det tilført 49 millioner hjemmesider, og ved utgangen av 2010 fantes det mer enn en billion sider tilgjengelig på internett – mer enn 150 sider per levende person på jorden. Det ble gjennomført mer enn fire milliarder søk hver dag (Hjeltnes & Warmedal, 2012, s. 88).

Næringslivets Sikkerhetsråd (NSR) har som formål å forebygge kriminalitet i og mot næringslivet. Et av virkemidlene er å informere om de kriminelle og sikkerhetsmessige truslene/trendene som eksisterer, men også formidle hva som forventes å skje i fremtiden. De siste åtte årene har de foretatt en mørketallsundersøkelse for å kartlegge omfanget av datakriminalitet og IT-sikkerhetshendelser. Verdien av sensitiv informasjon og truslene mot skjermingsverdig informasjon øker, og tiltak for å redusere sårbarheten utvikles ikke i samme takt (NSR, 2012, s. 4). Hovedfunnene i mørketallsundersøkelsen viser at trusselbildet er økende, noe journalister bør ta på alvor, og dette mest av alt med tanke på kildevernet.

Problemstilling

I lys av denne utviklingen har jeg valgt følgende problemstilling for oppgaven.

> *Hvordan ivaretar journalister kildevernet i dagens digitale samfunn, og tar de tilstrekkelig hensyn til informasjonssikkerhet?*

Jeg vil fokusere på følgende forskningsspørsmål.

- *Setter moderne kommunikasjonsløsninger kildevernet på prøve?*
- *Hvordan ivaretar journalister datasikkerheten når de frykter at de blir overvåket?*
- *Er kildevernet truet i dagens digitale samfunn?*

Denne oppgaven er et casestudie hvor jeg kommer til å intervjue journalister som mener de har blitt utsatt for dataangrep/hacking. Jeg kommer til å gå i dybden på konkrete caser hvor journalister kan ha blitt utsatt for denne kriminelle handlingen, og hvordan de mener å ha oppdaget ugjerningen. Et av kravene i Vær Varsom-plakaten er å ikke oppgi kildens identitet når kilden selv ber om anonymitet. Dersom man har dårlig datasikkerhet eller ikke tar tilstrekkelige overvåkningshensyn under kommunikasjon med kildene kan kildevernet kompromitteres. Som Svein Brurås (2010) sier: ”Vil kildene tørke ut dersom kildebeskyttelsen ikke er absolutt”. Tillitsforholdet mellom publikum og media er derfor essensielt for at viktig samfunnsinformasjon skal kunne se dagens lys, og ikke holdes skjult hos befolkningen. Det er derfor essensielt at journalister ivaretar nødvendige sikkerhetshensyn når de kommuniserer med kildene, men også at de sikrer sine data på en tilfredsstillende måte.

Det er ingen som vet hvordan de digitale sporene vi legger fra oss i samfunnet vil kunne brukes mot oss i fremtiden. Det lagres store mengder data både hos Internett-leverandørene og teleselskapene med flere. For journalister som jobber med sensitiv informasjon hvor kildene skal holdes anonyme kan dette få store konsekvenser. Med mange nye medier og nye måter å lagre informasjonen på, settes det også større krav til informasjonssikkerheten. I dagens mediesamfunn er alt som er tilknyttet Internett innen rekkevidde for utenforstående personer med vonde hensikter. Internett er ett og samme

nettverk, og det er bare spørsmål om kreativitet, ferdigheter og attraktivitet som avgjør om kriminelle klarer å få tak i informasjonen de jakter på.

Hva er datakriminalitet? – Noen begrepsavklaringer

I denne avhandlingen bruker jeg en del begreper som ofte flyter over i hverandre. Med begrepet datakriminalitet mener jeg som Petter Gottschalk, forfatter av boken *Datakriminalitet i Norge* (2011) sier i forordene av boken sin: "Å benytte informasjons- eller kommunikasjonsteknologi til å gjennomføre ulovlige handlinger, og dermed handler det om straffbare forhold". Politiet har også samme definisjon på datakriminalitet som Gottschalk sier i innledningen av boken sin. "Datakriminelle utnytter mulighetene som ligger i teknologien, til å begå lovbrudd. Disse kriminelle handlingene foregår ofte på Internett, og da kalt cyberkriminalitet" (politiet, datakriminalitet).

Typiske former for datakriminalitet er datainnbrudd, databedrageri, informasjonsheleri, skadeverk, dokumentforfalskning, og piratkopiering. Datainnbrudd er at noen trenger seg inn i andres datasystemer for å skaffe seg tilgang til beskyttet informasjon. Dette er en straffbar handling selv om man ikke har gjort seg kjent med informasjonen. Man kan skaffe seg uberettiget tilgang på mange forskjellige måter, for eksempel ved å misbruke passord eller utnytte sikkerhetshull. Når man utfører dataangrep er det vanlig at gjerningspersonen utfører en del kommandoer inne i datamaskinen han har koblet seg til (ibid.).

Datakriminalitet henger nesten alltid sammen med angrep mot informasjonssikkerhet. Det finnes en rekke metoder for å bryte seg inn i datasystemer utenfra, og dette blir stadig mer og mer utbredt. Informasjonssikkerhet er samlebetegnelsen for krav til påliteligheten og sikkerheten som knyttes til informasjon. Datasikkerheten er altså informasjonssikkerheten for informasjon som er lagret digitalt (Store norske leksikon, informasjonssikkerhet).

Den mest brukte betegnelsen om kriminelle på Internett er kanskje hackere. Da betegnelsen dukket opp for over 20 år siden, mente man personer som gjorde innbrudd uten å stjele. Hackerne gjorde det for å kunne skryte av det og legge igjen spor sier Gottschalk (2011) i innledningen av boken sin. Senere har hacking blitt forbundet med

andre former for kriminell aktivitet, inkludert profittmotiverte forbrytelser. Hacking blir ofte omtalt som programmering og operasjoner som krever en større IT-kompetanse enn gjennomsnittet.

Det mangetydige begrepet overvåking

Ordet overvåking er sentralt i denne oppgaven, men det kan virke noe diffust hva som ligger i begrepet. Jeg har derfor sett på hvordan begrepet benyttes og defineres. Overvåking forbindes for de fleste av oss med noe negativt. I rapporten til Lund-kommisjonen defineres begrepet på følgende måte "Aktive tiltak med sikte på å kartlegge en person, gruppe eller organisasjons holdninger eller virksomhet – så som avlytting ved bruk av tekniske hjelpemidler, ransaking av hus, skygging eller spaning, infiltrasjon eller aktiv bruk av informanter" (Bye & Sjue, 2008, s. 506). Begrepet overvåking benyttes med andre ord som betegnelse på visse metoder som brukes ved innhenting av opplysninger. Jeg kommer først og fremt til å fokusere på dagens moderne samfunn, og de digitale sporene journalister legger i fra seg. Dette fører blant annet til at kildene kan avsløres gjennom omfattende overvåking.

Redegjøring for litteraturen

I teoridelen har jeg hovedsakelig tatt utgangspunkt i litteratur som omhandler moderne overvåking. Her er boken *Overvåket* av Ronald Bye og Finn Sjue sentral. For å forstå hvordan man legger fra seg digitale spor og hva man må være oppmerksom på som journalist, har jeg brukt boken *Digitalt kildevern* av Anders Brenna, som for øvrig også er en av mine informanter. Kildevernet er også sentralt, og dermed har boken *Etikk for journalister* av Svein Brurås en sentral rolle. For å få et annet perspektiv på kildevernet har jeg også benyttet boken *Massemedias kildevern* av Ina Lindahl som er advokat med medierett som spesialisering. Datakriminalitet og datasikkerhet er viktige tema i avhandlingen, og jeg har da ikke kunnet unngå å bruke litteratur som går mer inn på den tekniske delen av avhandlingen.

Ettersom det er gjort lite forskning verden over om temaet har det vært utfordrende å finne litteratur som har relevans for tematikken i avhandlingen. Med god hjelp fra både veileder og kontakter innenfor media føler jeg at sammensetningen av litteraturen samsvarer godt med problemstillingen. Det er brukt mye nettkilder i oppgaven, og ettersom dette er et tema som er rykende ferskt på mange måter er nettkildene

ferskvare. Både litteraturvalgene og tolkningene jeg har gjort kan ha blitt preget av min forståelse av de digitale utfordringene i samfunnet. Det er jo et bevisst valg at litteraturen jeg har plukket ut til denne oppgaven samsvarer med mine tanker om tematikken. Jeg mener at litteraturen skal samsvare godt til problemstillingen, samtidig som jeg har problematisert fordeler og ulemper fra ulike sider.

Disponering av oppgaven

Mitt hovedfokus har vært å disponere oppgaven kronologisk slik at man forstår hvordan ny teknologi utfordrer måten journalister jobber på. Det har imidlertid vært vanskelig å sortere ut hva man skal fokusere på innenfor temaene: kilder, fra analog overvåking til Internett og datakommunikasjon og nettverk. Den tematiske inndelingen har vært krevende, og mange av temaene går til tider over i hverandre for senere å komme tilbake. Dette er ikke en oppgave som skal være belærende for journalister slik at de kan beskytte seg selv mot digitale farer. Det er mer en avhandling om de destruktive sidene i informasjonssamfunnet.

Kapittel 2 gir en oversikt over kilder og dens betydning for journalistikken. Med demokrati og ytringsfrihet er pressen talerøret for befolkningen. Noen ganger må journalistene bruke anonyme kilder av flere årsaker. Jeg drøfter også om kildevernet er satt under press som en følge av teknologien.

Kapittel 3 starter med hvilke ulike typer overvåking man kan bli utsatt for som journalist. Her gjør jeg et historisk tilbakeblikk på to av norgeshistoriens mest kjente overvåkningssaker av journalister. Moderne overvåkning har mange likheter med gårsdagens, og dette kommer jeg nærmere inn på, sett opp mot journalistenes kildevern. Etter dette tar jeg en gjennomgang av endringen Internett har hatt for både arbeidspraksisen til journalistene samt de usynlige truslene man nå står ovenfor. Mørketallsundersøkelsen til Næringslivets Sikkerhetsråd er sentral for å forstå at verden er i stadig endring. Her kommer jeg også inn på noen kjente datainnbrudd som er gjort mot norske og utenlandske medier ved hjelp av datakriminalitet på Internett.

Kapittel 4 går mer teknisk inn på noen av farene ved Internett. Jeg tar en gjennomgang av nye medier som mange av oss til daglig bruker både privat og på jobb som for eksempel PC, nettbrett og mobiltelefon. Her får man også et innblikk i hva det er viktig å

forstå for å unngå at noen kan spore eller utføre datainnbrudd. Til slutt går jeg gjennom nye trusler for datasikkerheten og kildevernet. Avslutningen handler om kjente datainnbrudd for å sette perspektiv på det som er gjennomgått tidligere.

Kapittel 5 er metodekapittelet med beskrivelser av hvilke fremgangsmåter jeg benytter meg av for å belyse problemstillingen. Her har jeg redegjort for de metodiske valgene og begrunnelsen for dem.

Kapittel 6 omhandler analysen hvor jeg diskuterer resultater og funn fra den kvalitative undersøkelsen.

Kapittel 7 er det avsluttende kapittelet om drøfting og konklusjon. Dette er en oppsummering av temaene jeg har dekket i den foregående fremstillingen, noe som fører til konklusjonen hvor jeg redegjør for de sentrale poengene og resultatene i undersøkelsen min.

Kapittel 2: Kilder

Ytringsfrihet

For å forstå pressens rolle i samfunnet kommer man ikke utenom menneskene og rettighetene vi har i demokratiet. Her er det viktig at man forstår ytringsfrihetens betydning som er grunnlovsfestet i §100, samtidig som den blir sett på som en svært sentral rett den norske befolkningen har. Med friheten til å formidle og motta tanker, meninger eller informasjon regnes ytringsfriheten som helt nødvendig i et demokratisk samfunn. Som Svein Brurås sier: ”Det grunnlovfestede vernet om ytringsfriheten er den viktigste presseloven vi har” (2010, s. 19). Dette sier mye om hvilken rolle media har i samfunnet, og det er derfra betegnelsen den fjerde statsmakt har sitt opphav.

Siden 1999 har Den europeiske menneskerettskonvensjonen (EMK) hatt status som gjeldende rett i Norge (Lovdata, menneskerettsloven). Det vil si at konvensjonen ble en del av norsk lov. EMK skal ved motstrid gå foran bestemmelser i annen lovgivning. Dette innebærer i praksis at EMK får trinnhøyde mellom grunnloven og den formelle lovgivningen (Lindahl, 2009, s. 39). Ytringsfriheten blir vernet av EMKs artikkel ti som

lyder slik: ”Frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser” (ibid.). Befolkningen skal ha lov til å ytre seg, uten å måtte frykte for represalier, og pressens kildebeskyttelse sikrer i en del tilfeller denne retten. Som Brurås hevder: ”Viktig samfunnsinformasjon vil aldri se dagens lys, den vil forbli skjult for offentligheten. Derfor hender det at journalistene lover kilder anonymitet” (Hjeltnes & Warmedal, 2012, s. 321). Jeg vil med utgangspunkt i ytringsfriheten se på journalisters forhold til befolkningen.

Reporterens kildenett

For journalister handler mye av jobben om å ha kontakt med verden utenfor redaksjonslokalene. Sakene man jobber med er ofte svært forskjellige slik at man hele tiden må kunne omstille seg raskt for å kunne ta nye avgjørelser. ”Journalistikk er *valg* – valg av idé/problemstilling, valg av kilder, valg av kildeutsagn, valg av vinkling, valg av presentasjonsform, sjanger, bilder og illustrasjoner” (Østlyngen & Øvrebø, 2006, s. 16).

Det er derfor viktig at journalister har kontakt med mennesker ansikt til ansikt for å bli kjent med folk innenfor profesjonelle rammer. Man skal ikke være venner med kilden, og kildene skal ikke være journalistenes oppdragsgivere. Et relevant kildemateriale kan svare på, eller bidra til å svare på, våre spørsmål, våre antagelser og vår hypoteser. Enhver beboer i det norske demokratiet skal kunne utrykke det de ønsker og mener, uten risiko for straff. Man trenger åpenhet rundt samfunnsprosesser, og det er pressens oppgave å videreformidle dette videre fra kilder og ut til befolkningen. ”Journalisten har satt navnet ”*kilder*” på sine kontaktpersoner, nettopp fordi de er *kilder til informasjon*. (Østlyngen & Øvrebø, 2006, s. 133). Det som formidles skal være riktig, og det skal formidles slik at publikum innser at det er riktig og viktig.

> Pressens troverdighet er nært knyttet til journalisters og redaktørers integritet. Skal publikum ha tillit til en journalist, må de være trygge på at journalisten er uavhengig og fri i sin journalistiske virksomhet, uten bindinger til kilder eller maktsentra utenfor redaksjonen, og at journalisten ikke har personlige interesser å ivareta gjennom sin virksomhet (Brurås, 2010, s. 54).

Det finnes mennesker som ønsker å hindre fri informasjonsformidling og fri adgang til kildene. For mange kan interessen for å påvirke journalistene være stor slik at de får publisert det som tjener kilden. Østlyngen og Øvrebø gir følgende råd mot å unngå

kildestyring : "Journalisters beste vern mot kildestyring er å sikre seg et bredt kildenett. Men i tillegg må hun – og redaksjonen også tåle straffen det kan medføre å ha gode kunnskaper og mange kontakter på et felt. Mektige kilder kan på ulike måter forsøke å holde en journalist utenfor (2006, s. 134).

Kildekritikk

Som Svein Brurås sier i boken *Etikk for journalister,* er to av de viktigste kjennetegnene innenfor journalistikken fritt kildevalg, og den kritiske holdningen journalistene har til kildene. Kvaliteten på det arbeidet som journalistene gjør avhenger derfor i stor grad av kildens kvalitet (Brurås, 2010, s. 121). Vi er alle mennesker av kjøtt og blod som sitter med informasjon eller observasjoner som kan være av interesse for media. Som mennesker har vi både sterke og svake sider, og motivene for å offentliggjøre noe i media kan være mange. Det er journalistens ansvar å finne frem til de gode kildene.

Definisjonen for en *kilde* er: "Enhver som gir opplysninger til representantene fra pressen. Opplysningene kan være fakta, meninger eller ideer fremlagt i form av tekst, tale og eller bilde" (Lindahl, 2009, s. 13). I Vær Varsom-plakaten punkt 3.1 kommer det tydelig frem at hovedregelen i journalistikken er at kildene skal identifiseres. "Kilden for informasjon skal som hovedregel identifiseres, med mindre det kommer i konflikt med kildevernet eller hensynet til tredjeperson" (Norsk Presseforbund).

Kildene er en hjørnestein for journalister, og en nødvendighet for at publikum skal ha troverdighet til informasjonen som massemedia publiserer. Det er mange samfunnsaktører som har stor interesse av å bruke media til å publisere informasjon de er tjent med, men disse aktørene er også opptatte av å hindre publiseringer av informasjon som kan gi dem negativ oppmerksomhet. Det er mediene sin oppgave å velge ut hvilke kilder som skal benyttes i saken, og det er derfor svært viktig at man ikke gir etter for presset fra dem som ønsker å hindre en åpen debatt. En viktig rolle for journalistene er derfor at man har en kritisk holdning til kildene som ønsker å dele informasjon med media, og det materiale som legges frem. Dette ses på som en forutsetning for all journalistikk og heter på fagspråket *kildekritikk*. Vær Varsom-Plakaten sier følgende:

> 3.2. Vær kritisk i valg av kilder, og kontroller at opplysninger som gis er korrekte. Det er god presseskikk å tilstrebe bredde og relevans i valg av kilder. Vær spesielt aktsom ved behandling av informasjon fra anonyme kilder, informasjon fra kilder som tilbyr eksklusivitet, og informasjon som er gitt fra kilder mot betaling (Norsk Presseforbund).

Det er journalisten sitt ansvar å kontrollerer at opplysningene som gis er korrekte. Det betyr at informasjonen fra en kilde i utgangspunktet skal bekreftes av en annen kilde for å verifisere kildens versjon av historiene. "Dersom journalisten bringer videre en uriktig opplysning fra en kilde, så er dette journalisten sitt ansvar" (Brurås, 2010, s. 118). Publikum bør vite hvem som innestår for uttalelsene fordi de selv skal kunne bedømme hvilken vekt de skal tillegge opplysningene. For at saken skal være troverdig er det stor forskjell på om det er en ekspert som uttaler seg eller en synser. Utgangspunktet for journalister er derfor at de ikke skal tro på alt som blir sagt, og informantene må derfor sjekkes og kontrolleres. Åpenhet er viktig, og bredde i kildevalg og dokumentasjonen er en styrke i journalistikken.

Anonyme kilder

I en del situasjoner kan ikke kilden stå frem i pressen med navn eller bilde dersom den viktige informasjonen skal publiseres for offentligheten. Når man møter en kilde som man har gitt et løfte om anonymitet, er det klart at det er mange farer når man ser det fra et kildekritisk synspunkt. Det er jo ikke dagligdags at man har behov for å love kilder anonymitet, men i enkelte tilfeller kan de være den eneste måten journalisten kan skaffe seg informasjon på. Det er ikke uproblematisk å bruke anonyme kilder. Fossum og Meyer mener at: "Problemet er at den avtalte anonymiteten forandrer opphavssituasjonen drastisk, og krever kildekritisk oppmerksomhet" (2008, s. 119).

Det er jo uten tvil positivt at journalisten får tilgang på informasjon som ellers ville vært utilgjengelig. Når det gjelder negative sider er det trekk ved denne opphavssituasjonen som ikke bare påvirker det som blir sagt, i retning av sannferdighet (ibid.). Kilden trenger dermed aldri å stå til ansvar for det som har blitt sagt. I boken om *Presseetikk fra a til å* står det følgende om å bruke anonyme kilder i journalistikk:

> På den ene siden fører bruken av anonyme kilder til at viktige opplysninger, nemlig hvem som sa hva, blir holdt unna publikum. Det kan føre til at den

> offentlige debatt som nettopp pressen ønsker å stimulere/beskytte, kan bli skadelidende fordi publikum ikke kan forholde seg til opplysninger om navngitte kilder. I slike situasjoner står også redaksjonene i fare for å bli brukt av personer som slipper å stå ansvarlig for sine synspunkter for offentligheten (Bodahl-Johansen, 1996).

Lover man en kilde anonymitet så holder man det 100% (Brurås, 2010, s. 178). Dersom kildene holdes anonyme kan det likevel åpne opp for uheldige bindinger eller skjult påvirkning. Det kan være mange grunner til at kildene ønsker å forbli anonyme, og ikke ønsker å stå frem i offentlighetens søkelys. Det finnes flere måter å gjengi informasjonen fra anonyme kilder på: "kilde i forsvaret", "en ansatt ved skolen" eller "en person fra regjeringskvartalet" osv. I noen tilfeller er det helt nødvendig at kildene forblir anonyme for å unngå konflikter etter publisering. "Det skjer dessverre litt for ofte at kilder som står frem offentlig med kritikk, blir straffet for det i ettertid" (Brenna, 2012, s. 16-17). Dersom man ikke er anonym, kan det at man står frem i media føre til: baksnakking, ødelagte karrieremuligheter, refs fra leder, utestenging fra fellesskapet, eller at man blir fratatt arbeidsoppgaver.

Det er gjort undersøkelser på hvilke områder innenfor journalistikken det brukes flest anonyme kilder. Det kommer tydelig frem at det er innenfor *utenriks* og *kriminalstoff* (Lindahl, 2009, s. 19). Dersom man melder fra om kritikkverdige arbeidsforhold som allmennheten bør vite om vil man naturligvis være engstelig for reaksjonene fra ledelse og kollegaer. For kilder som går offentlig ut med informasjon om kriminelle miljøer kan hevn være noe man frykter mest. Løfter om anonymitet får ofte kilden til å vise stor åpenhet, men fra et kildekritisk synspunkt innebærer dette en risiko fordi informanten slipper å stå til ansvar for mulige feil i fremstillingen.

I saken om Watergate-avsløringen i 1974 førte den anonyme kilden *Deep Throat* til at president Richard Nixon gikk av som president i USA. Den anonyme kilden ga umåtelig bistand til journalistene Bob Woodward og Carl Bernstein som jobbet for New York Times. Avisen avdekket skritt for skritt hvordan personer i valgkomiteen til Nixon hadde organisert et innbrudd i demokratenes hovedkvarter, Watergate. Den hemmelige kilden fremstår som en av de mest langvarige journalistiske mysterier noensinne. I 2005 sto kilden selv frem med nyheten om at han var den mystiske *Deep Throat*. Det var den

tidligere nestsjefen i FBI Mark Felt som hele livet hadde klart å holde dette skjult for offentligheten (VG. 31.05.2005).

For journalistene er det altså svært mange fallgruver når man bruker anonyme kilder, men kildevernet er absolutt, og et brudd på dette svekker tiltroen til hele pressen. I dagens teknologisamfunn setter dette nye krav til informasjonssikkerheten til journalistene. Ifølge Østlyngen og Øvrebø sa tidligere generalsekretær i Norsk Redaktørforening Nils E. Øy følgende om ikke å bli misbrukt av anonyme kilder: "Lag et notat der du skriver ned alt det kilden forteller deg. Deretter ber du kilden skrive under og bekrefte at den versjonen du skriver er riktig – fremdeles under løfte om kildebeskyttelse" (2006, s. 299).

Kildevern

Med kildevernet har journalistene rett til å nekte å oppgi hvem som er kilden til viktige opplysninger i en sak. Som journalist kan man ikke pålegges å oppgi kildens identitet eller utlevere informasjon som avslører kilden. "Etter krigen har det aldri skjedd at en journalist eller redaktør har etterkommet pålegg fra en domstol om å oppgi en kilde" (Brurås, 2010, s. 179). Det er altså utenkelig for en journalist å oppgi en kilde som i all fortrolighet er lovet anonymitet. Man skal ikke under noen omstendigheter oppgi kilden ved å etterkomme pålegget fra domstolen. Vær Varsom-plakaten sier følgende:

> 3.4. Vern om pressens kilder. Kildevernet er et grunnleggende prinsipp i et fritt samfunn og er en forutsetning for at pressen skal kunne fylle sin samfunnsoppgave og sikre tilgangen på vesentlig informasjon.
>
> 3.5. Oppgi ikke navn på kilde for opplysninger som er gitt i fortrolighet, hvis dette ikke er uttrykkelig avtalt med vedkommende.

For hardtarbeidende journalister som jobber med gravejournalistikk kan den nye teknologien føre til at kildejegerne klarer å spore kilden. I dag er det skremmende få journalister som har gode kunnskaper om overvåkning. Slik ble gårsdagens overvåkning og etterretning behandlet, og slik blir dagens nye overvåkning behandlet. Det redaksjonelle grepet om dagens elektronisk baserte kartlegging, sporing og overvåkning er svakt (Bye & Sjue, 2008, s. 468). Det at man kan avlyttes eller bli overvåket er ikke noe nytt. Med nye medier og store mengder data som lagres finnes det uante muligheter

for å finne informasjon som kan brukes i en eventuell kildejakt.

Både kilder og journalister legger fra seg langt flere spor nå enn før Internett var et faktum, men også overvåkingen ellers i samfunnet har økt. Dersom beskyttelsen av varslerne i årene fremover er sviktende kan det bety at pressen får flere tips fra anonyme kilder som ikke tør å kontakte sin arbeidsgiver, fagforening eller andre aktører for å melde fra om kritikkverdige forhold (Brenna, 2012, s. 12). Vi trenger modige journalister og varslere som fungerer som vaktbikkjer utenfor de formelle organene. Hva ville journalistikken vært uten avsløringer av kriminelle forhold, og annen viktig samfunnsinformasjon? Den journalisten som bryter kildevernet ødelegger mye for seg selv og andre i yrket.

Dersom man jobber som gravejournalist må man beherske mange ulike teknologier og metoder samtidig som man har en god digital grunnforståelse. "Undersøkende journalister som lykkes, arbeider hyre målrettet og systematisk, og de blir ofte utsatt for press og motstand" (Hjeltnes & Warmedal, 2012, s. 13). Med en verden i stor elektronisk utvikling er det ganske åpenbart at anonyme kilder kan være langt mer utsatte og sårbare enn tidligere. En av grunnene til dette er at man med enkle metoder kan overvåke både mobiltelefon og nettbrettet til svært mange uvitende samfunnsborgere. Det trenges stort mot og en sterkere beskyttelse for kildene enn hva tilfellet er i dag. For arbeidsgivere, privat som offentlig, på jakt etter en anonym kilde blant sine ansatte, er det store muligheter å avsløre hvem han eller hun er ved hjelp av elektroniske spor. Dette kommer jeg nærmere tilbake til senere i oppgaven.

Det finnes ikke noe måte man kan sikre informasjonen eller kildene sine på hvor man kan føle seg helt trygg på at ingen prøver å få tak i informasjonen man besitter. I en undersøkelse utført av TNS Gallup kommer det frem at vi bryr oss svært lite om informasjonssikkerhet. Under halvparten av oss er opptatte av informasjonssikkerhet noe som kan føre til at sensitive opplysninger kommer på avveie. I en tid da stadig mer informasjon deles og stadig flere medier tas i bruk er dette urovekkende, sier Tore Orderløkken ved Norsk senter for informasjonssikring (NorSIS 09.09.2010). Det er enkelt å tro at journalister er mer opptatt av datasikkerhet enn folk flest, men dette er det vanskelig å finne gode holdepunkter på. Hvordan kan en journalist love kilden

anonymitet hvis kommunikasjonen mellom dem og informasjonen som lagres ikke er trygg?

Kildevernet er svært viktig for journalister som jobber med gravejournalistikk og bruker anonyme kilder i sakene sine. Både irrasjonelle og rasjonelle krefter kan reagere med ekstraordinære tiltak dersom de oppdager at de er i ferd med å bli avslørt. Desto viktigere er det at allmennheten stoler på at pressen ivaretar kildevernet på en god måte uten å måtte være redd for at uvedkommende kan avsløre kontakten mellom journalist og kilde. Finn Sjue sier følgende om dagens journalister:

> Jeg er redd for at det store flertallet av journalister i Norge fortsatt har svake kunnskaper om de ulike formene som overvåkingen kan ta. Det gjelder både generelt og som tiltak rettet mot journalister, redaksjoner, kilder og varslere. Naiviteten rår dessverre grunnen. Jeg sier ikke dette for å fornærme en hel yrkesgruppe, men fordi jeg mener det er til skade for maktkritisk journalistikk. Vi må vende et blad (Sjue, 2011, s. 134).

I dagens samfunn er svært mye informasjon digital, og dette har endret måten journalistene jobber og kommuniserer på. Man legger fra seg elektroniske spor overalt, men det er også enklere for kildene å komme i kontakt med journalistene. Det er viktig at journalistene forstår at dette kan brukes til å avsløre kildene. Det er lett å skremme journalister med eksempler på hva som er mulig for utenforstående å gjøre dersom de har tilgang på digitale spor, men det er ikke hensikten. Kildevernet er under konstant press og det er enhver journalists plikt å ivareta det. Finn Sjue og Ronald Bye sier: ”At den nye overvåkingen – i motsetning til gårsdagens overvåking – er av en slik natur at ingen kan unngå den. Den nye overvåkingen angår derfor både deg og meg, oss alle” (2008, s. 11). Jeg skal videre drøfte hvorfor moderne teknologi og datasikkerhet kan være en trussel for journalister.

Kapittel 3 – Fra analog overvåking til Internett

For å forstå bakgrunnen for at mediehusene står ovenfor *usynlige* trusler utenfra i form av datakriminalitet, er det viktig å se hvordan den teknologiske verden vi lever i har endret seg drastisk de siste tjue årene. Med nye medier følger også nye måter å drive overvåking på som er langt mer teknisk avansert enn gårdagens. Det er fortsatt mange

av de samme metodene som brukes, men i dagens digitale samfunn er den elektroniske overvåkingen blitt regjerende. Helt siden Internett gjorde sitt inntog i 1991 har datamaskinen blitt et viktig arbeidsverktøy for mennesker verden over. Store mengder data lagres, og lokal lagring har gått mer og mer over til nettskyetjenester. Dette er tjenester hvor man kan lagre data slik at de er tilgjengelige fra hele verden. For journalister er det et slående trekk ved nettbruken at den er variert og preget av individuelle mønstre. Noen har faste morgenrutiner, der de leser et fast utvalg nettaviser for å skaffe seg overblikk over dagens nyhetsbilde. Noen lar NTB sette dagsorden for å finne egne vinklinger på saker, mens andre igjen bruker nettet til åpne søk (Ottosen & Krumsvik 2008, s. 177).

Verden er mindre en noen gang, og med Internett som et verdensomspennende nettverk kan man finne informasjon om det aller meste. Arbeidsverktøyene til journalistene har gått fra den tradisjonelle notatblokken og telefonen til datamaskin, smarttelefon og nettbrett med Internett-tilgang. Notatblokken lever i høyeste grad fortsatt, men måten man oppbevarer det journalistiske stoffet og kommuniserer med kildene på har endret seg. Mediene har de siste tjue årene gjennomgått store endringer når det gjelder hvordan man publiserer nyheter og når ut til publikum. Med en ny generasjon mediebrukere har papiravisen og TV gått mer og mer over til Internett. Det er på Internett det skjer og man er ikke lengre avhengig av tid og sted for å få med seg sine favoritt TV-serier eller se nyhetene. ”Vi er nå vitne til flere parallelle utviklingstrekk som vil påvirke mediemarkedet i årene som kommer. Avisenes papiropplag synker, og det tradisjonelle avismedium har problemer med å trekke til seg nye lesere” (Ottosen & Krumsvik 2008, s. 13). Forvandlingen skjer fort og medievanene endres i takt med ny teknologi som inntar forbrukermarkedet. Den digitale verden har for lengst inntatt journalistikken, og omveltningene har vært mange for å tilpasse seg ett nytt mediemarked i stadig endring.

På Internett har alle mediene blitt samlet, og med smarttelefoner og nettbrett har mediene konvergert. Det vil si at det som tidligere var et medium som telefon, radio eller TV nå er tilgjengelig i et og samme medium. Når teknologi smelter sammen, legges grunnlaget for ulike bruksmåter (Ottosen & Krumsvik 2008, s. 79). Uansett hvilket medium man jobber for, er det viktig at man sikrer informasjonen sin på en god måte.

Med så mange medier og kommunikasjonskanaler setter det nye krav til journalistene for hvordan de oppbevarer informasjonen sin på. Mediebildet har endret seg fra at journalistene formidler informasjon til at det nå er mye mer toveiskommunikasjon både på sosiale medier og e-post. De digitale sporene som legges igjen kan brukes til å finne ut hvem kilden er, men også til å overvåke journalistene som jobber med viktige nyhetssaker. Spørsmålet er hva dette betyr for journalistenes arbeidsdag når det gjelder informasjonslagring og kildevern.

Ulike typer overvåking

For å forstå hva overvåkning er ønsker jeg å gå nærmere inn på ulike måter dette kan foregå på. Det er mulig å overvåke uten å bryte loven som for eksempel ved ren observasjon. Politiet kan også overvåke, og har egne metoder hvor de har tilgang til systemer der det er lagret informasjon om oss. Det er også mulig å overvåke ulovlig ved at man for eksempel hacker eller avlytter noen. Overvåkingen starter oftest ved at det samles inn omfattende informasjon om oss. Dette kan gjøres på mange måter enten man bruker ren observasjon, forfølger en person over tid eller velger å samle inn informasjonen elektronisk. Man kan overvåke gjennom menneskelig eller teknisk observasjon, muntlig overlevering, det skrevne ord eller elektronisk ved at alle elektroniske spor vi legger igjen etter oss blir lagret.

> De ulike formene for overvåking kan skje mer eller mindre automatisert, mer eller mindre intenst, og på ulike nivåer – fra det enkle til det komplekse. De elektroniske og automatiserte formene for overvåking er i ferd med å skyte kraftig fart (Bye & Sjue, 2008, s. 53).

Så lenge opplysningene om oss er lagret noe sted, kan de brukes som utgangspunkt for overvåking. Dette kan gjøres gjennom for eksempel å avlytte telefonsamtaler eller overvåke de elektroniske samtalene våre på chat eller e-post. Ved å bruke moderne teknologi er mulighetene mange og produktene lett tilgjengelige for å drive ulovlig overvåking.

I denne oppgaven kommer jeg til å konsentrere meg om ulovlige måter å drive overvåkning på ved å se på hvordan Internett og moderne teknologi kan brukes til å komme seg inn på journalistene og mediehusene sine medium. Dette gjøres for eksempel for å sabotere, spionere, stjele data eller finne kilden i en stor nyhetssak.

Jeg vil se nærmere på hvordan myndigheter, politiet, og private interesser kan ta i bruk moderne teknologi til å overvåke. Dagens overvåkning er ikke ulik gårsdagens og jeg ønsker først å ta et historisk tilbakeblikk for å se på overvåkning i et historisk perspektiv. Den kjente norske journalisten Finn Sjue ble overvåket av norske myndigheter i en årrekke da han var redaktør i klassekampen tidlig på 70-tallet.

Historisk tilbakeblikk på overvåking av journalister

Det er nå over tretti år siden den kjente Ikkevolds-saken fant sted hos avisen Ny Tid. Etter nattlige razziaer og endeløse rettsaker mener de sentrale aktørene i saken at forsvaret fikk det som de ville med en mindre kritisk presse (Ny Tid, 19.06.2004). Gjennom razzia i lokalene til avisen og tiltale ville Politiet skremme bort journalister fra å drive med gravejournalistikk i forhold til Forsvaret og sikkerhetspolitikken. Saken handlet om at avisen hadde skrevet en artikkel om en lyttestasjon for ubåter på Andøya, og de ble beskyldt for å spre forsvarshemmeligheter. Forsvaret tapte saken og avisen ble frikjent, og dermed ble noen grenser flyttet i forhold til hva som er tillatt å skrive om. Etter dette ble det innført et forbud mot innsyn for politiet. «Endelig kan nevnes at det i relasjon til pressen er spesielt viktig at Politiet ikke får adgang til andre opplysninger enn de etter loven har adgang til å skaffe seg» (ibid.).

Etter 1990 har det vært vanlig å karakterisere hele perioden fra ca. 1945 til ca. 1990 som den kalde krigen (Store norske leksikon, Den kalde krigen). I denne perioden overvåket E-tjenesten her hjemme en rekke norske borgere og deriblant journalister. De drev altså med ulovlig virksomhet, og dette førte til et kraftig oppgjør om hemmelighold og lovstridig overvåkning. Stortinget satte derfor i 1994 ned en kommisjon for å granske påstander om ulovlig overvåkning av norske borgere. Kommisjonen ble ledet av høyesterettsdommer Ketil Lund, og kommisjonen er derfor kjent som Lund-kommisjonen.

De rettet søkelyset særlig mot Arbeiderpartiets dominans, og i 1996 kunne kommisjonen dokumentere en serie med overtramp og lovstridig overvåking (Sjue, 2011, s. 136). Det var NKP-ere, SF-ere og til slutt AKP-ere som hadde blitt overvåket og terskelen for overvåking var svært lav. Politiets overvåkingstjeneste (POT) fikk gjennomgå, og dette førte til at 379 personer fikk erstatning. En av disse var daværende

redaktør i Klassekampen, Finn Sjue, som ble overvåket i 16 år av norske myndigheter. Sjue, som er utdannet psykolog, har vært både redaktør og gravejournalist.

Sjue var sentral i Palestina-arbeidet og han satt i den daglige ledelsen av AKP samtidig som han var redaktør for Klassekampen. Han omtaler det hele som lite trivelige opplevelser, og opplevde overvåkingsmetodene som patetiske og primitive. For Sjue ble det ikke bare et personlig ubehag men også et stort press. For han ble det en trussel mot seriøs gravende journalistikk. Han visste at han og kollegaene ble overvåket på ulikt vis og overvåkingsmetodene som ble brukt var spaning og telefonavlytting både hjemme og på jobb. Etter Lund-kommisjonens rapport ble de store mørke rommene i politikk og forvaltning ikke lenger fredet på samme måte som under den kalde krigen. POT lå med brukket rygg og samspillet mellom pressefolk og tjenestene fortsatte, men i dels i svært anstrengte og nye former (Sjue, 2011, s. 138).

Sjue peker på to av de største problemene med overvåkingen: ”Slitasjen på redaksjonen og det aller viktigste nemlig risikoen som kildene ble utsatt for”. Det skapte store komplikasjoner for redaksjonen og det ble nesten alltid vanskelig å føre samtaler med kildene. ”Det måtte mye tid, oppfinnsomhet og kreativitet til for å drive kildesamtaler utenfor redaksjonslokalene” (Bye & Sjue, 2008, s. 36). Det var utrolig mange kilder som ble utsatt for risiko og ubehag, men Sjue mener han gjorde det han kunne for å beskytte kildene. Som redaktør hadde han mange samtaler med kilder som var knyttet til politiet, militæret eller internasjonale grupper og organisasjoner. I ettertid førte dette til bekymringer for om kildene kunne ha blitt utsatt for en risiko og skade fordi møtene og samtalene ble overvåket. Jeg kommer videre til å ha fokus på nye overvåkningsmetoder og at det i dag er langt flere aktører som kan benytte seg av overvåkning.

Som Finn Sjue sier i boken *Undersøkende journalistikk en innføring* (2011, s. 139) handler det å bli overvåket om to store spørsmål:

1. *Redaksjonell integritet*: Å forsvare redaksjonens rett til og mulighet for å skaffe seg bredt innsyn i kritikkverdige forhold.

2. *Kildebeskyttelse*: Å beskytte viktige kilder og varslere, de som gir redaksjonen innsyn i kritikkverdige forhold.

Moderne overvåkning

I en verden hvor man er overvåket fra mange hold er det naivt å tro at ingen der ute kan se oss. Journalister er selvfølgelig ikke mindre utsatt enn andre yrkesgrupper, og det har vært kontroversielle situasjoner med både avlytting og spionasje på journalister tidligere både her til lands og i utlandet. Dette er ikke noe forsøk på å skremme journalister fra å bruke nye medium. Det handler mer om å bevisstgjøre seg selv på om at man jobber med sensitiv informasjon, og måten man behandler denne på handler mye om tilliten journalister har til befolkningen. Dersom noen får tak i informasjonen svekker det tilliten til journalistene, og det kan få store følger for personene det gjelder. Forfatteren bak boken *Digitalt kildevern* Anders Brenna sier følgende:

> Det er litt som med Lotto. Det er usannsynlig at jeg vinner i Lotto fordi sjansene er så små, men det er sannsynlig at noen vinner fordi det er så mange som spiller. Det er noen som vinner hver uke, og slik er det også med muligheten for å bli overvåket. Noen vil helt sikkert oppleve det, spørsmålet er hvem (2012, s. 11).

Det er derfor svært viktig at journalister og ikke minst de som graver i sensitive saker, forstår hvordan de moderne formene for overvåkning fungerer. Hvilke krefter er det som benytter seg av den, og hvordan kan redaksjoner og journalister og deres kilder overvåkes?

> ”Det burde vært en obligatorisk opplæring ved enhver journalistutdanning i Norge. Men så er ikke tilfelle. Det burde også vært en del av medienes interne opplæring. Men så langt jeg kjenner til forholdene i medier flest, er heller ikke det tilfelle” (Sjue, 2011, s. 139).

Så sent som i 2013 overvåket forsvaret norske journalister ulovlig ved å drive kartlegging, så kanskje er ikke den statlige overvåkningen av norske journalister et avsluttet kapittel likevel? Journalistene hadde i flere år drevet kritisk journalistikk om de hemmelige tjenestene i landet. Sjefsredaktør i VG, Torry Pedersen, mener dette er uakseptabelt av Forsvaret og at de korrekte etiske og samfunnsmessige vurderingene ikke har slått inn (TV 2, 21.03.2013).

Det er ikke bare det å beskytte kildene media har måttet endret fokus på de siste årene. Kriminelle hackere tilbyr nå å sabotere pressen gjennom såkalte cyberangrep. Dette er en global trend som det finnes en rekke eksempler på også her til lands. Hackerne pøser på med informasjon mot mediehusene og setter dem dermed ut av drift. Det er billig å få utført slike dataangrep og derfor er informasjonssikkerhet essensielt. Gruppen *Komiteen for beskyttelse av journalister* mener dette er en global trend (Dagens Næringsliv 15.02.2013). Dette er synlige angrep som er enklere å spore enn andre hackerangrep ettersom skadene er synlige i form av at nettavisene faller ut, eller at noen endrer innholdet på sidene. De fleste hackerangrepene er skjulte og gjennomføres profesjonelt ved at man skjuler sporene etter seg.

Ifølge Bye & Sjue (2008, s. 53) er det i dag særlig fire samfunnsmakter som bedriver elektronisk overvåkning:

- Staten og dens spesielle organer og tjenester
- private selskaper, bedrifter, konserner og institusjoner
- private nettverk som primært driver med organisert kriminalitet
- fremmede makter

Mørketallsundersøkelsen - Informasjonssikkerhet og datakriminalitet

Næringslivets Sikkerhetsråd har som hovedformål å forebygge kriminalitet i og mot næringslivet. De skal informere om kriminelle trusler og trender som er aktuelle, og som forventes å komme i fremtiden. I mørketallsundersøkelsen som er gjennomført elektronisk av TNS Gallup presenteres det fakta om IT-tilstanden i privat og offentlig næringsliv i Norge. Det var totalt 886 virksomheter som svarte på undersøkelsen. Ifølge ny forskning er Norge verdens mest teknologisk avanserte land når det kommer til digitale medier. For mange av oss starter dagen med smarttelefonen eller nettbrettet i hånden. Vi har blitt avhengige av å følge med på hva som skjer i nyhetsbildet og på sosiale medier, sa tidligere multimediadirektør i TV 2, Hege Kosberg (TV 2, 14.02.2012).

Mange har god økonomi og kan derfor kjøpe seg det nyeste på teknologifronten. Det satses tungt fra mediebransjen for å møte den teknologiske utviklingen. Dette setter nye

krav til informasjonssikkerheten hos bedriftene for å gjøre dem mindre sårbare for datakriminalitet. Hele 62% av norske virksomheter svarer at det er kritisk dersom IT-systemene er nede inntil en dag. IT-avhengigheten og truslene øker, men det er en synkende sikkerhetsbevissthet i norske virksomheter. Noe av grunnen til dette er de manglende styrings- og registreringssystemer av datakriminalitet som bedriftene har. De har ikke oversikt over angrep eller systemer som er sikre når det utvikles nye måter å begå datainnbrudd på. Det er mange virksomheter som tar i bruk ny teknologi uten at de foretar risikoanalyser og etablerer retningslinjer. Dette gjør virksomhetene særlig sårbare for sikkerhetshendelser. Det er bare 24% av virksomhetene i undersøkelsen som krypterer bærbare media, og det er 29% av virksomhetene som har retningslinjer for sikker bruk av mobiltelefon.

I tabellen nedenfor kommer det tydelig frem hvor få det er som anmelder IT-kriminalitet. Underrapporteringen fører til et uriktig kriminalitetsbilde. Den viktigste årsaken til dette synes å være at virksomheten ser på hendelsen som ubetydelig. Dette henger sammen med at de tror det er umulig å finne gjerningsmannen og at angrepet ikke var rettet mot deres virksomhet. På Nasjonal sikkerhetsmyndighets (NSM) konferanse i 2011 var datakriminalitet tema. Justis- og beredskapsminister Grete Faremo sa følgende da hun åpnet konferansen: "Vi må ta inn over oss at den virtuelle verden er blitt høyst reell. IKT er i dag integrert i de fleste områder i samfunnet" (NSM 17.11.2011). Faremo sa også at Norge ønsker å møte utfordringene med å utvikle et elektronisk Politi slik at man kan følge elektroniske spor bedre enn hva tilfellet er i dag.

Type hendelse	Estimat	Anmeldelser
1) Datainnbrudd (hacking)	3 200	144
2) Dataskadeverk og – bedrageri	33 000	
a. Uautorisert endring/sletting av data	2 300	
b. Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten	900	143
c. Bedrageri ved misbruk av kredittkort over internett	29 800	
3) Misbruk av IT-ressurser	2 600	47
4) Spredning av ulovlig/opphavsrettslig beskyttet materiale	5 900	0
5) Tyveri av informasjon	100	27
Totalt	**44 800**	**361**

Estimatene er basert på opplysningene fra årets undersøkelse, samt SSBs statistikk over næringsstrukturen i Norge fordelt på antall ansatte.

Figur 1: Rapporterte anmeldelser fra Mørketallsundersøkelsen 2012

I Mørketallsundersøkelsen kommer det frem at det er større gap nå en tidligere mellom trusler og sikkerhetstiltak blant norske virksomheter. Dette skjer parallelt med at IT-avhengigheten øker. Mye av grunnen til dette er at ledere mangler kunnskap om informasjonssikkerhet, og at de heller ikke har oversikt over trusler og farer som kan være svært skadelig for bedriften. Dette kan være noe av forklaringen på at mange virksomheter ikke har tatt i bruk tilgjengelige sikkerhetstiltak og heller ikke har fokus på sikkerhetskultur (ibid.).

Bruk av privateid utstyr til virksomhetsinformasjon er økende. Dette medfører en større risiko ettersom utstyret brukes i mange sammenhenger og på en rekke forskjellige nettverk, noe som gjør det vanskeligere å beskytte seg mot angrep. Det er stor økning ved bruk av e-post på mobiltelefoner og aktiviteten på sosiale medier øker, men bedriftene mangler retningslinjer. Annette Tjaberg som er assisterende direktør i NSM sier at mobiltelefoner, sosiale medier og nettbrett har gjort oss mer sårbare enn noen gang. "Mørketallsundersøkelsen viser at sikkerheten er sviktende, og at det er få tegn til forbedring, sier Tjaberg" (Aftenposten 16.11.2011).

Mediebransjens sikkerhetsutfordringer

I en verden hvor man er overvåket fra mange hold er det naivt å tro at ingen der ute ser oss. Lite tyder på at journalister er mindre utsatt enn andre yrkesgrupper i samfunnet. Dette er ikke noe forsøk på å skremme journalister fra å bruke digitale medier, men det handler om å bevisstgjøre seg selv om at man jobber med sensitiv informasjon. Måten man behandler informasjonen på er med på å forsterke tillitten til befolkningen. Dersom noen får tak i informasjonen blir tilliten svekket, og det kan få store følger for personene det gjelder. Det er derfor svært viktig at journalister som graver i sensitive saker forstår hvordan de moderne formene for overvåking fungerer. Hvilke krefter er det som benytter seg av overvåkningen, og hvordan kan journalister, redaksjoner og deres kilder overvåkes?

Datainnbrudd

Det finnes en verden der ute som er usynlig og fjern for de fleste av oss. Vi har alle hørt om dem som utgjør en trussel for både privatpersoner og bedrifter, nemlig hackerne. På

filmene fremstilles de ofte som personer som sitter bak svarte skjermer med grønn skrift. Datainnbrudd er noe kjent men samtidig noe de færreste av oss har noe forhold til før ugjerningen finner sted. Mange av oss beskytter seg med antivirusprogram og brannmur, og på denne måten føler man en slags *falsk* trygghet. Dersom man er tilknyttet Internett er man på samme nettverk som alle andre verden over. Da kan man i teorien være et mulig offer for datainnbrudd. Du og din virksomhet er utsatt for trusler og farer du knapt har hørt om, og dette er ikke noe som er i ferd med å avta. "Datainnbrudd, tjenesteavbrudd, fortrolig informasjon på avveier, forfalsket informasjon og andre uheldige hendelser relatert til informasjonssikkerhet er slett ikke i ferd med å forsvinne – de mangedobles og forsterkes" (Daler, Gulbrandsen, Høie, Sjølstad, 2010, s. 23). Du eller din virksomhet kan være neste offer, uten å vite hva som har skjedd. Jeg skal videre se på noen kjente dataangrep mot media både i Norge og i utlandet.

Datakriminalitet mot norske nettaviser

I mai 1999 hacket to 18-åringer hjemmesiden til Aftenposten, og fikk rekordstreng straff for skadene de påførte. De hadde erstattet den opprinnelige nettsiden med et bilde av tre menn som urinerte på Aftenpostens logo. De ble avslørt av politiet og saken ble anmeldt. De fikk henholdsvis 45 og 29 dager ubetinget fengsel samt en bot på 4000 kroner. Dette var første gang man brukte den strenge bestemmelsen i datainnbruddslovens § 145, tredje ledd, som innebærer betinget fengsel, opplyser etterforsker Arild Lyssand fra Økokrims IKT-gruppe i Informasjons- og kommunikasjonsteknologi til Aftenposten (VG, 24.01.2001).

Det at nettsider har blitt angrepet er noe som har fulgt med Internett fra dens begynnelse. Trend Micro er et internasjonalt sikkerhetsselskap som har overvåket en rekke russiske hackerforum og deretter laget en oversikt over hva det koster å få utført forskjellige typer dataangrep. Man kan med andre ord bestille målrettede angrep på Internett dersom man ønsker å spionere, stjele eller sabotere en nettside (Trendmicro, 2012). Bak et slikt angrep kan det stå ansatte, tidligere ansatte, kunder, kildejegere, eller en hacker som gjør dette fordi det er en utfordring. Dette kan enten være ren sabotasje, eller en måte å skjule et målrettet hackerangrep på hvor formålet er noe annet enn bare å sabotere selve nettsiden.

Denne typen dataangrep kalles tjenestenektangrep (Denial of Service, ”DoS”) som handler om ulike former for angrep med det formål å stoppe eller delvis ødelegge en tjeneste, eventuelt et datanettverk hos en leverandør eller virksomhet (Daler et al., 2010, s. 401). Det innebærer at angrepene kommer fra forskjellige steder i verden ved at hackerne bruker PC-ene til fremmede personer til å angripe nettavisens hjemmeside med så mange forespørsler at den til slutt bryter sammen. Et slikt angrep kan man bestille for 10 dollar og angrepet varer da i en time. For en hel dags angrep mot et nettsted koster det 30-70 Dollar (Trendmicro, 2012, 101, s. 4).

Slike angrep har rammet norske nettaviser en rekke ganger og også fått nettsidene til å bryte sammen i perioder når angrepene har vært kraftige nok. På kvelden den 10.02.2010 ble både VG.no og Dagbladet.no angrepet. I løpet av kort tid ble nettstedene lastet ned hele 5000 ganger og dette førte til kollapsen. Utgavesjefen på nettsiden til Dagbladet, Eugene Brandal, forteller at: ”Klokken 19.30 begynte flere tyrkiske IP-adresser å laste nettsiden fem tusen ganger i løpet av en kort periode. Etter at den første bølgen med nedlastninger kom, har det i flere timer vært umulig å komme seg inn på Dagbladet.no” (Journalisten, 10.02.2010). Det er umulig å fastslå hva grunnen til slike angrep er, men de brukes ofte til å finne hull i sikkerhetssystemet sånn at hackerne kommer seg videre inn i datasystemene. Man kan heller ikke utelukke at det er for å sensurere pressen. Dagbladet hadde kort tid før angrepet publisert muhammedtegninger, noe som skapte store protester.

> For Dagbladet er det en fortvilet situasjon når slike ting inntrer. At noen med vitende og vilje går inn og saboterer våre nettsider som stopper publiseringen av nyheter er veldig alvorlig. Nå skal vi ha fakta på bordet og vil etter å ha gjennomgått dem vurdere hvordan saken skal forfølges, sier konstituert sjefredaktør, Lars Helle (ibid.).

Post- og teletilsynet (PT) har kartlagt og vurdert sikkerheten og stabiliteten ved det norske toppdomenet .no, som forvaltes av UNITETT Norid AS. På noen områder er det pekt på tiltak som kan forbedre prosesser og ivareta sikkerheten. Ytterligere, men samlet sett er PT meget godt fornøyd etter sikkerhetsgjennomgangen av hele Norids virksomhet (Post- og teletilsynet, 2012). Dersom Norid blir angrepet og satt ut av spill kan det få enorme konsekvenser ettersom de har kontrollen på alle .no domenene til norske virksomheter. Jeg vil nå vise til et eksempel fra USA og avisen New York Times

om hva hackere er i stand til å gjøre slik at man forstår hvilke konsekvenser dataangrep kan få for media.

Datakriminalitet mot New York Times

New Tork Times publiserte den 25. oktober 2012 en artikkel med følgende overskrift "*Billions in Hiddden Riches for Family of Chinese Leader*". Det var en kritisk artikkel om formuen til den kinesiske statsministeren Wen Jiabao og hans familie. Samme dag opplevde avisen et massivt angrep fra kinesiske hackere. Ifølge sikkerhetseksperter er det funnet bevis for at passordene til samtlige av de 1150 redaksjonelt ansatte ble stjålet. Deretter ble passordene brukt til å bryte seg inn på 53 datamaskiner, de fleste av dem var utenfor redaksjonslokalene. Blant annet ble e-postkontoen til avisens Shanghai-kontor hacket (ITavisen 31.01.2013). Dette er altså en av USAs største aviser som ble overvåket over en lang periode. Det er lite som tyder på at hackerne har fått ut e-poster eller annen informasjon som er knyttet til Wen-saken.

IT-ekspertene er sikre på at angrepene stammer fra det kinesiske militæret (ibid.). Angrepene startet fra de samme datamaskinene, og metodene er de samme som har vært brukt til dataangrep mot USA hvor man tidligere har slått fast at det kinesiske *cyberforsvaret* står bak. Gjennom avsløringene til New York Times hvor de tar for seg de store økonomiske interessene statsministerfamilien har i kinesiske selskaper med lukrative statlige kontrakter, utalte kinesiske diplomater at dette kom til å få konsekvenser. Den 20. februar publiserte nettsikkerhetsselskapet Mandiat en rapport der det kommer frem at en rekke dataangrep lar seg spore til en tilsynelatende vanlig bygning i den kinesiske storbyen Shanghai (Mandiat, 2013). For det kinesiske utenriksdepartementet Hong Lei sier at det er svært vanskelig å spore såkalte cyberangrep tilbake til opprinnelsen. Han tilbakeviser anklagene om datainnbrudd, og ser på det som uansvarlig og unødvendig å beskylde regjeringen i Beijing for å stå bak dataangrepene på USA (Dagbladet, 19.02.2013).

Det er vanskelig å si hvem som står bak hackingen, og de er gode til å skjule sporene de legger fra seg. Marie Moe som er seksjonssjef for NSM kjenner godt til rapporten og forteller at angrepene blir mer sofistikerte og at det er tydelig at angriperne har store ressurser. Hun sier at rapporten til Mandiat er et solid stykke arbeid og at trendene er de samme i Norge (ibid.). For selskapene dette gjelder er det i midlertidig fatalt å gå ut

offentlig med informasjon om at man er kompromittert, og de fleste ofrene blir derfor en godt bevart hemmelighet. Hva betyr slike angrep for kildevernet når plutselig utenforstående får full tilgang inn i mediehusenes datasystemer? Jeg skal nå se nærmere på teknologien som er utsatt for datainnbrudd og kriminelle handlinger.

Kapittel 4 - Datakommunikasjon og nettverk

Internett

Dette verdensomspennende datanettverket danner basisen for en rekke kommunikasjonstjenester. Man kan i praksis få tilgang til alt som er tilkoblet Internett dersom man selv er tilknyttet. Dette er jo positivt på mange måter, men det stilles større krav til brukerne når det gjelder sikkerhetsplanlegging og oppfølging av sine medium. De som står bak et dataangrep trenger ikke å ha kjennskap til virksomheten eller nettets arkitektur, selv om kjennskap til virksomheten vil gjøre det enklere for hackerne å få tilgang (Daler et al, 2010). Arbeidet med å utarbeide sikre løsninger for Internett pågår hele tiden ettersom truslene endres fra dag til dag. Virksomheter bør ikke ta i bruk Internett før sikkerhetsforholdene knyttet til bruken er nøye vurdert, og relevante og nødvendige tiltak er iverksatt. Som Bye & Sjue sier: ”Det er fullt mulig å juble over den nye teknologien, og samtidig gråte blod over de destruktive sidene den kan ha” (2008, s. 51). Det er enkelt å være tilhenger av moderne teknologi og listen over positive sider i det digitale samfunnet er lang når man ser på alle fordelene teknologien fører med seg.

Kablet nettverk vs trådløst nettverk

Innenfor datanettverk er det enten snakk om et kablet eller trådløst nettverk. Med et kablet nettverk er du mer usynlig ettersom nettverket ikke er like synlig for offentligheten som det trådløse nettverket. Det kreves vanligvis fysisk tilgang til kabelen for å bryte seg inn på det kablede nettverket. På et trådløst nettverk kan hvem som helst se nett-trafikken, og det er derfor man bør bruke kryptering. Kryptering er noe som gjør dataene uleselige for andre enn den rettmessige mottakeren. Det er ikke 100% sikkert, men det styrker sikkerheten betraktelig. Passordene til det trådløse nettverket kan også knekkes, og i tillegg finnes det alltids en eller annen svakhet i systemet. Men betyr dette at et trådløst nettverk er enklere å komme seg inn på enn de tradisjonelle kablede nettverkene? Geir Kalleberg er direktør i Datametrix, en ledene leverandør av løsninger

som muliggjør sikker kommunikasjon på Internett. Han sier følgende: ”Både trådløse og kablede nett kan være både sikre eller usikre. Ikke skyld på teknologien. Det er hvordan man bruker den, og hvordan man tenker, som avgjør om du har sikre nett eller ikke” (International Data Group, 23.01.2012).

Kalleberg sier også at det vil være relativt enkelt for en dreven sosial hacker, på engelsk kalt (*social engineering)*, å komme seg inn på et kablet nettverk. Med dette menes at man får tilgang til det kablede nettverket ved å lure noen til å få tilgang innenfor veggene hvor nettverket er. Jeg kommer til å gå nærmere inn på dette litt senere. Når det gjelder de trådløse nettverkene er de fleste klar over at det er mer utsatt for datainnbrudd, slik at man er mer oppmerksomme på dette.

På den andre siden stoler man for mye på sikkerheten på kablede nettverk, men tester viser at det er mye lettere å komme seg inn på de kablede nettverkene enn de trådløse fordi man stoler for mye på den fysiske sikkerheten (ibid.). Det er altså ikke noen nettverk som er 100% sikre, men det at man er bevisste på farene og tar forholdsregler ved å gjøre en grundig sikkerhetsgjennomgang med påfølgende tiltak gjør at man kan lagre dataene på en tryggere måte. Man skal altså forsøke å skape god og nødvendig sikkerhet i et usikret medium som i prinsippet er åpent for alle.

Medium

PC/Bærbar og stasjonær

Norge ligger på verdenstoppen når det gjelder antall PC-er i forhold til innbyggertallet (TV 2, 16.12.2011). De aller fleste PC-er som benyttes i arbeidssammenheng utenfor bedriftens sikre soner, inneholder informasjon som uvedkommende ikke må få tilgang til. Harddiskene er store nok til at man kan lagre ekstreme mengder bilder, musikk, video, og tekst. PC-ene inneholder også mengder av e-post, dokumenter og andre ting du slett ikke vil skal havne på avveie. Stasjonært datautstyr installert innenfor virksomhetens sikkerhetsarkitektur erstattes i økende grad av bærbare PC-er som tilkobles virksomhetens nettverk (ibid.).

Det er mange ansatte som benytter de samme PC-ene på jobb som hjemme, og dette skaper problemer for sikkerheten. Sikkerhetstiltakene som gjelder for bruk av datautstyr innenfor de sikre sonene til redaksjonene, bør også gjelde når det teknologiske utstyrer brukes utenfor virksomheten. Forhåpentligvis er sikkerheten god nok til at eventuelle hackere ikke få tilgang til selve informasjonen som ligger lagret. Det er ledelsens ansvar at PC utstyret og annet mobilt datautstyr sikres tilstrekkelig.

Det er også mange som får en falsk trygghet av å bruke mac og tror at de ikke er så utsatte for datakriminalitet som PC-brukerne. Men i takt med den økende popularitetet er nå mac-maskiner mer utsatt for datainnbrudd (Hardware, 30.07.2009). Det er oppdaget feil i mac sin programvare som gjør det mulig for angripere å ta kontroll over dine data. Det er uvanlig at hackerne klarer å komme seg inn på mac-maskiner, men sikkerhetseksperter mener dette kommer til å endre seg nå som det er vanligere å benytte mac. Ifølge Miller og Dai Zovi (2009) som er forfatter til boka "*The mac hacker´s handbook*" OS X som er operativsystemet til mac til å bli like utsatt som Windows når de kriminelle retter mer fokus på systemet. Dette er kanskje en pekepinn i ett samfunn hvor man til stadighet hører at det ikke er nødvendig med virusprogram fordi du har mac.

Nettbrett

Et nettbrett er en mellomting mellom en smarttelefon og en bærbar datamaskin. Først kom lesebrettene for å lese tekst, så ble de mer avanserte slik at det er mulig å vise bilder, se video, høre på musikk og surfe på Internett. Man kan stort sett gjøre det samme som på en datamaskin. Det mest kjente nettbrettet er iPad fra Apple, men Samsungs og andres modeller har også blitt svært populære de siste årene. Populariteten til nettbrettet har nok sammenheng med dets mange bruksområder. Det er i dag over en million nordmenn som har kjøpt nettbrett, og det har vært en eksplosiv vekst (Online, 01.06.2012).

Nettbrettene er små, lette og enkle å ta med seg når man er på farten. Dermed er også sjansen for å glemme, miste eller få de stjålet tilstede. De inneholder ofte mye sensitiv informasjon, og det er derfor viktig at nettbrettene tilbyr nye sikkerhetstiltak som fjernsletting av data og passordbeskyttelse. Mobilitet og sikkerhet bør være en av de største utfordringene og prioriteringene for norske virksomheter (Aftenposten

06.04.2011). Det må altså stilles nye krav til sikkerheten med den økende bruken av nettbrett og smarttelefoner som gir mye større mobilitet.

Sikkerhetsselskapet Watchcom har testet sikkerheten på de fire største operativsystemene som de ulike nettbrettene bruker. Testen konkluderte med at iPad er det tryggeste nettbrettet å bruke på jobben. Det kommer ferdig kryptert ut av esken og det er de strenge godkjennelsesprosedyrer for apper som gjør at mange av sikkerhetsutfordringene håndteres på en god måte. De mener autentisering, kryptering og sikker kommunikasjon er kritisk for sikkerheten på nettbrett. Eirik Saltkjel som er sikkerhetsrådgiver i Watchcom sier at skillet mellom jobb og privat informasjon gjerne smelter sammen på nettbrett for de fleste brukerne. "Nettbrettet deles i mye større grad med andre, siden det brukes til arbeid og underholdning både hjemme og på farten (ibid.). Mange bedrifter opplever det nok som problematisk at nettbrettene blir kjøpt inn privat hos ansatte. Dette gjør det vanskelig for bedriftene å vite om deres data er sikre, og brukerne vet nødvendigvis ikke hva de kan, eller må gjøre for å ivareta sikkerheten på nettbrettet sitt.

Mobiltelefon - Telefon

Telefonen var en gang en revolusjon for kommunikasjonen mellom mennesker. Med mobiltelefonen sitt inntog var man plutselig tilgjengelig overalt døgnet rundt. Det som en gang bare var en telefon man kunne ta med seg har nå blitt en *mini-pc* med de samme mulighetene som en datamaskin. Smarttelefonen, eller touchtelefonen som dagens mobiltelefoner også kalles, har blitt allemannseie og telefonene er proppet med personlig informasjon. 90% av alle telefoner som selges i dag er smarttelefoner med Internettilgang. Norge og nordmenn er en mobil-nasjon som konsumerer mer og mer av sitt daglige Internett-innhold via mobile enheter (Aftenposten, 06.04.2011).

Journalister vandrer rundt med lomma full av sensitiv informasjon som altfor lett kan havne i feile hender. "Personlig informasjon kan være «framtidens valuta». Det kan selges, og være verdifullt for mange. Det er viktig å sikre denne informasjonen, sier Guro Skåltveit, senior informasjonsrådgiver i Datatilsynet" (TV 2, 02.03.2013). Når hackeren først er inne på telefonen din kan den egentlige eieren raskt låses ute. Når man i tillegg

gjerne har stilt inn telefonen til å huske både passordene til Facebook og E-post er det mye sensitiv informasjon som kan havne hos feil personer.

> Vi må være bevisste på hva det er vi går rundt med i lomma. I tillegg til private bilder og Facebook-kontoer med automatisk passordhusking, er det mange som bruker telefonen som et arbeidsredskap. Viktige dokumenter og sensitiv informasjon ligger ofte dårlig sikret i smarttelefonen vår, sier Skåltveit (ibid.).

Digital kildejakt

Gjennom Internett og de nye mediene jeg har beskrevet legger vi fra oss store mengder digitale spor. Dette er ikke noe man til daglig går og tenker på ettersom sporene er usynlige. Sporene kan benyttes i en kildejakt, og det dukker stadig opp nye metoder for å finne sporene og samle dem. At man legger fra seg mange digitale spor er det liten tvil om, men dette oppdager man kanskje ikke før man selv er bevisst på det. Jeg kommer videre til å se litt på noen elementer som kan være nyttig å tenke på som journalist i en hektisk arbeidshverdag.

IP-adresse

Alle enheter som er knyttet opp mot Internett har en unik IP-adresse. For en hacker er dette en av de viktigste opplysningene man kan sikre seg for å gjøre et datainnbrudd. Hackerne kan være ute etter IP-adressen til e-postserveren, webserveren eller datamaskiner på nettverket. Når man har funnet IP-adressen til en av enhetene ovenfor er det ofte enklere å finne IP-adressene til de andre serverne eller PC-ene på nettverket.

”IP-adressering er bruk av IP-adresser for å identifisere enheter i et nettverk. En slik enhet kan være en PC, skriver eller en annen enhet som har sin egen IP-adresse som er unik, for eksempel 128.121.188.201” (Daler et al., 2010, s. 361-363). Dette er ofte det første en hacker leter etter når han skal utføre en kriminell handling. Har man adressen til vedkommende er det avhengig av sikkerheten om hackeren klarer å få tilgang eller ikke. På samme måte som man har innbruddsalarm og dørlås på huset, er det like viktig at man sikrer sine data ved hjelp av for eksempel virusprogram, brannmur og kryptering.

E-post

Journalister sender og mottar mange e-poster daglig. Dette er en åpen kanal og en rask måte å kommunisere på, men den er også svært utsatt og kan være en stor

sikkerhetstrussel. På e-posten har man ofte lagret mye sensitiv informasjon som kan misbrukes dersom den kommer på avveie. Det er også mange av oss som lagrer brukernavn og passord til andre tjenester på e-posten, noe som kan få store konsekvenser dersom andre får tilgang til e-post kontoen din.

Noe som er kjent for de fleste av oss er SPAM-post som er en fellesbetegnelse på all e-post som er uønsket (ibid.). Slike meldinger kan inneholde skjulte hensikter, ofte med formål om å svindle, lure eller skremme mottakeren. En veldig kjent metode er at man mottar e-poster med infiserte vedlegg. Dette kan være et word-dokument, bilde eller en PDF-fil som inneholder relevant informasjon for mottakeren. Dette kan føre til at man blir lurt til å åpne innholdet, og da kan et sikkerhetshull utnyttes slik at et trojansk overvåkningsprogram installeres uten at journalisten vet om det. Så lenge det ikke er noe krav om signering av e-post som kan fortelle hvem som er avsender, er dette problemer vi må leve med. Det er kun vår bevissthet og forsiktighet som vil forhindre oss i å bli lurt.

Kunnskapsrike hackere og innsamlingsfasen

Det er lett å få inntrykket av at det er dataspesialister som sitter og koder på en svart skjerm som begår datakriminalitet. Det er ofte slik man har sett det på film, men det er ofte de enkle metodene som gjøre at hackerne får tak i den sentrale informasjonen de trenger for å bryte seg inn i datasystemer. Det er ikke tilfeldig at mange hendelser, både i virkeligheten og i hackerromaner, tar utgangspunkt i å gjette passord, forsøke å knekke dem ved hjelp at dataprogrammer eller først og fremst *social engineerin*g (Hardware, 27.06.2004). Det handler om at man prøver å lure noen til å rette oppmerksomheten mot feil sted, får så å hente ut informasjon eller lure seg inn. Dette er en helt annerledes måte å angripe datasystemene på. På samme måte som gravejournalister på jakt etter informasjon finner mange løse tråder som til slutt fører til et svar, kan altså hackere begå kriminelle handlinger.

Kevin Mitnick, som er en av verdens mest kjente hackere, anser sjarm som den viktigste egenskapen for en hacker (Daler et al, 2010, s. 70). Dette gir et innblikk i at en hacker nødvendigvis ikke er den mest datakyndige personen, men også en detektiv. En måte å få tak i nødvendig informasjon på kan være så enkelt som at man kommer seg inn i bygningen hvor journalisten er. Dette kan gjøres ved at man står utenfor og leser en avis

eller trykker på mobiltelefonen, for så å gå inn med de andre ansatte når de er ferdige med røykepausen. Man kan også utgi seg for å være rengjøringspersonell eller vekter for å komme seg inn i bygningen uten at noen ansatte stiller spørsmålstegn til hvem personene er. Hackeren kan da gå og lete etter for eksempel passord på kontorpulter mens de ansatte spiser lunsj, eller se om det er noen som ikke er logget av på PC-en slik at man får direkte tilgang til innholdet på datamaskinen.

Det svakeste leddet it IT-sikkerhet

Når man skal lage et IT-system så sikkert som mulig, handler det ikke bare om å minimere risikoen for datainnbrudd, men man må finne balansen mellom sikkerhet og brukervennlighet. Dersom man hele tiden tenker sikkerhet ender man opp med at medarbeidere ikke vil bruke IT-systemet. Det er mennesker som er det svakeste leddet i IT-sikkerheten, sier Christian W. Probst, førsteamanuensis ved Danmarks Tekniske Universitet. Han mener følgende: ”Når hackerne først har kommet seg inn i IT-systemet via en medarbeidernes PC, har de som regel lett adgang til å rote rundt i deler av bedriftens data” (Forskning.no, 08.11.2012).

Probst påpeker at det eneste en hacker trenger for å komme seg inn på datasystemene er en person som ikke kjenner bedriftens sikkerhetspolitikk til punkt og prikke. I forskningen til Probst fokuserer han på adgangskontrollen til både mennesker og programmer. Han spør etter hvilke muligheter aktøren har i IT-systemer og hvilke konsekvenser disse mulighetene har. Han mener at dette er et oversett ledd i datasikkerheten til virksomhetene (ibid.).

Nettskytjenester

Nettskyer som også blir kalt *Cloud Computing* som er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet Internett (Datatilsynet, 18.12.2012). Mange eksterne serverparker står utenfor Norges grenser, og det er en utfordring for virksomhetene å sørge for at avtalene er i samsvar med norsk lovgivning. Man har altså tilgang til data på alle enhetene man bruker, som for eksempel smarttelefon, nettbrett og bærbar-PC. Det eneste du trenger for å koble deg til nettskyen er en enkel programvare, brukernavn og passord. En slik tjeneste kan gi mer fleksible og integrerte løsninger. Dette er praktisk,

men det byr på en rekke utfordringer for brukerne og bedriftene som bruker nettskytjenester.

> Bruk av nettskytjenester reiser også en rekke spørsmål knyttet til beskyttelse av data som behandles i løsningen. Det vil kunne være økt risiko at kunden mister kontroll over personopplysninger og at kunden ikke har fullstendig informasjon med tanke på hvem, hvor og hvordan dataene blir behandlet. For kunder som behandler personopplysninger bør det velges en leverandør som garanterer overholdelse av EUs personvernlovgivning (Brenna, 2012, s. 106).

I mørketallsundersøkelsen i informasjonssikkerhet og datakriminalitet fra 2012 brukte nesten halvparten av virksomhetene (46%) en eller annen form for nettskytjeneste. De vanligste tjenestene er iCloud, Dropbox og og Gmail. Bare 9% svarer at de har utarbeidet retningslinjer for bruk av nettskytjenester. Dette skaper nye utfordringer for å beskytte seg mot inntrengere som er på utkikk etter dine data.

Datalagringsdirektivet

Det mye omtalte Datalagringsdirektivet (DLD) ble vedtatt i Stortinget 4. april 2011 med et lite flertall som hovedsakelig bestod av stemmer fra Arbeiderpartiet og Høyre. Dette direktivet skal ha som formål å kunne brukes dersom etterforskning av terrorisme og alvorlig kriminalitet finner sted. På hjemmesiden til DLD står det følgende ”Datatilsynet er både tilsyn og ombud. Vi skal medvirke til at den enkelte ikke blir krenket gjennom bruk av opplysninger som kan knyttes til han eller henne” (Datatilsynet, 27.11.2011)

Ved å lagre digitale spor kan politiet finne ut hvem som har snakket med hvem, samt finne ut hvor vedkommende har vært frem til, og under handlingen. Tanken bak dette er i utgangspunkt svært god når man tenker på at vi lever i en verden hvor det stadig skjer kriminelle handlinger som oppklares ved hjelp av digitale spor. DLD skal lagre data om deg i seks måneder som blant annet innebærer, telefonsamtaler, sms-er, e-poster og IP-adresser. Innholdet i kommunikasjonen lagres ikke, men det lagres info om tid, sted og hvem man kommuniserer med i denne perioden. Dette kan være en måte å spore journalister og kilder i en eventuell kildejakt. I april 2014 så kjente EU-domstolen DLD som ugyldig. Dermed plikter ikke Norge lengre å innføre direktivet. Direktør i DLD Bjørn Erik Thon sa kort tid etter avgjørelsen følgende:

> Avgjørelsen sier tydelig at direktivet er et alvorlig inngrep i den enkeltes privatliv og kan avsløre detaljerte opplysninger om vårt privatliv, som for eksempel hva vi gjør, hvem vi omgås og hvor vi befinner oss. I tillegg kan den omfattende lagringen av tele- og Internettdata gi folk en følelse av å være kontinuerlig overvåket (Datatilsynet, 08.04.2014).

Ettersom Norge tidligere var pliktige i forhold til EØS-avtalen til å innføre direktivet, er det nå opp til regjeringen om vedtaket om å innføre direktivet fortsatt skal være gjeldende. Dermed må Norge ta stilling til om vi har noen av de samme svakhetene som EU-domstolen påpekte eller om de mener direktivet fortsatt er nødvendig.

Wikileaks

I 2007 grunnla den australske journalisten Julian Assange nettstedet Wikileaks. Hensikten med nettstedet var å lage et sikkert nettsted hvor man kunne publisere lekkede dokumenter gjennom sikker beskyttelse av kilder, journalister, varslere og aktivister, uten at kildene selv ble kjent. Ved å publisere klassifiserte eller konfidensielle dokumenter, utfordret Wikileaks de mektigste nasjonene i verden ved å gi offentligheten et eksklusivt innsyn bak kulissene til verdenspolitikken. De har stegvis publisert 251 287 ambassaderapporter fra det amerikanske utenriksdepartementet (Rosenbach, 2011, s. 7). I følge nettstedet selv består Wikileaks av en uavhengig global gruppe personer som kjemper for en fri presse og for mest mulig gjennomsiktighet i samfunnet. Dokumentene som Wikileaks publiserer skal ha politisk, diplomatisk eller etisk betydning.

> For Assange, men og for den amerikanske regjeringa lignet året 2010 et fyrverkeri. Desto lenger ut gjennom året en kom, desto mer spektakulære ble avsløringene. På slutten av året kom høydepunktet som fikk regjeringer over hele verden til å miste pusten (Ibid.).

De første årene publiserte Wikileaks alle dokumentene på sin egen nettside slik at alle kunne gå inn å lese dem. Med enorme mengder informasjon var det nesten umulig å orientere seg i jungelen av dokumenter. Fra 2010 endret de strategien ved å samarbeide med store mediehus som amerikanske New York Times, den britiske storavisen *The Guardian*, det tyske nyhetsmagasinet *Der Spiegel*, *franske Le Monde* og spanske *El Pais*. Aktivistene i Wikileaks bestemte seg for slippe litt informasjon om gangen ettersom

Assange til nå følte tilbakemeldingene og publiseringene hadde gitt mindre respons enn forventet. Med hjelp fra media og journalistisk med utsiling av informasjonen, fikk Wikileaks nå enorm oppmerksomhet verden over rundt publiseringene sine (Rosenbach, 2011, s. 98-99). Dersom Assange og hans nærmeste ble tatt, måtte dataene kunne åpnes raskt av andre og derfor var mediegigantene viktige støttespillere. Aftenposten fikk tilgang til alle de lekkede filene mot Assange sin vilje etter at en av personene som Assange hadde tillitt til, brøt samarbeidet. Dette sørget for at Aftenposten endte opp med verdens best krypterte sikrede filer som de hadde full tilgang til (Brenna, 04.01.2011).

Wikileaks er på ingen måte noen erstatning for journalistikken, men den har vært med på å endret den. Nyhetsredaktøren i Aftenposten, Erik Almlid, forteller at det er de samme nyhetskriteriene og kildekritikken som ligger til grunne for Wikileaks som for alle andre nyheter. ”Vi vurderer om det er interessant, og om det er hensyn som for eksempel til personvernet eller menneskers sikkerhet som gjør at vi ikke kan publisere materialet” (Aftenposten, 12.10.2011). Almlid mener sakene som er omtalt gjennom Wikileaks avsløringene er av vesentlig betydning for leserne. Dette er altså en stor utfordring for mediene som utfordrer offentligheten om hva slags informasjon som bør være skjult. Dette kan være med på å sette soldaters og kilders liv i fare. Den nye medieteknologien er med på å informere verden på en helt ny måte, gjennom tradisjonelle journalistiske metoder og prinsipper. Spørsmålet er hvilke konsekvenser det vil få?

Wikileaks mener at de kan garantere for kildens anonymitet ved at de krypterer informasjonen som kommer til dem. Assange sier de bruker avanserte teknikker for å beskytte kildene sine, og hans kunnskaper om kryptering strekker seg langt over de fleste. Lekkasjene har skapt sterke reaksjoner og den amerikanske administrasjonen mener det er uansvarlig og farlig å publisere de stjålne dokumentene som også er ufullstendig. Med slike fiender må IT-sikkerheten være så sikker som overhodet mulig (Brenna, 04.01.2011). Hvis informasjonen skal brukes til noe må man være sikre på at de som har dette lagret er tillitten verdig. Ethvert sikkerhetssystem kan i utgangspunktet hackes og her har selvsagt Aftenposten et stort ansvar for å beskytte sensitiv informasjon og kildene sine.

Edward Joseph Snowden

Snowden er en amerikansk IT-tekniker som jobbet for National Security Agency (NSA) da han lekket graderte opplysninger om det amerikanske etterretningsprogrammet PRISM til *The Guardian* og *The Washington Post* i juni 2013 (Harding, 2014, s. 9-14). E-posten som Guardian-kommentator Glenn Greenwald mottok var anonym, og begynte slik: ”Jeg er en betrodd mann i etterretningstjenesten”. Vedkommende sa ingenting om seg selv, og det kunne være hvem som helst slik at Greenwald hadde store problemer med å tro at e-posten var ekte. Det var ekstremt hemmelig hva NSA drev med, og det hadde aldri vært noen lekkasjer tidligere fra den amerikanske etterretningstjenesten. Snowden, som var anonym, sendte derfor noen oppsiktsvekkende hemmelige dokumenter til Greenwald (ibid.) Gitt at dokumentene var ekte, så det ut til at de åpnet for en verdensomspennende viktighet. Snowden sa blant annet følgende: ”Jeg vil ikke leve i en verden der alt jeg sier, alt jeg gjør, alle jeg snakker med, hvert eneste utrykk for kreativitet, kjærlighet eller vennskap, blir registrert” (Harding, 2014, s. 9).

Edward Snowdens avsløringer har berørt land i verden – også Norge. Man har fått vite mye om fremgangsmåtene til NSA. De overvåket ikke bare fiender men også venner og deriblant forbundskansler Angela Merkel. Det tyske nyhetsmagasinet *Der Spiegel* mener å sitte på opplysninger som viser at NSA har hatt tilgang til Merkels telefon helt siden 2002 (NRK, 26.10.2013). Tallene for Norge er oppsiktsvekkende. I løpet av en måned vinteren 2012/13 innhentet USA data om over 33 millioner norske telefonsamtaler. Reaksjonen fra politisk hold i Norge var anstrengt – og en noe forvirret Erna Solberg uttalte: ”Venner bør ikke overvåke hverandre” (Harding, 2014, s. 9). Av det som har kommet frem til nå har overvåkningen vært så omfattende at det for mange har vært vanskelig å forstå omfanget. NSA samlet inn data fra millioner av private e-poster, tekstmeldinger og telefonsamtaler.

Kapittel 5 - Metode og utvalg

I denne delen ønsker jeg å legge frem resultatene fra dybdeintervjuene jeg har gjort med fem norske journalister. Fire av journalistene mener å ha blitt utsatt for dataangrep. De har varierende IT-kunnskaper, men to av dem jobber i tillegg med IT som fagfelt. Anders Brenna (frilansjournalist og forfatter med IT-utdanning) og Espen Andersen (journalist, forfatter og programmerer i NRK Brennpunkt). De andre journalistene er Kristoffer Rønneberg (korrespondent for Aftenposten i New York, tidligere Beijing, Ole Erik Almlid (tidligere nyhetsredaktør i Aftenposten) og Kjetil Stormark (frilansjournalist og forfatter). Jeg ønsker å se på hvilke konkrete episoder disse journalistene mener å ha blitt overvåket eller utsatt for dataangrep, og til slutt hvordan de ivaretar kildevernet. Analysen er inndelt i fire hovedtemaer etter oppdelingen i intervjuguiden. Dataangrep, datasikkerhet, journalist-rollen samt den journalistiske praksisen og arbeidsmåten.

Utfordringer

Gjennom mine problemstillinger har jeg kommet frem til at en kvalitativ metodisk tilnærming vil være den beste fremgangsmåten for å gi dybdekunnskap om emnet jeg ønsker å beskrive. Jeg har en todelt problemstilling som er overlappende, men samtidig krever innsikt fra forskjellige typer informanter. Derfor har jeg også brukt to journalister med IT-utdanning som kan belyse dette temaet fra en annen side. Den første delen av problemstillingen søker å belyse hvordan journalister ivaretar kildevernet i dagens digitale samfunn. For å kunne belyse dette har jeg intervjuet noen av journalistene i Norge som mener de har blitt utsatt for et dataangrep. Gjennom intervjuer med disse journalistene har jeg ønsket å få et innblikk i hva som ligger til grunne for hvorfor de mener å ha blitt utsatt for dataangrep. Når det gjelder dokumentasjonen av at man har blitt utsatt for et dataangrep så er dette svært krevende.

Denne undersøkelsen i masteroppgaven skal forsøke å være et bidrag til å forstå at norske journalister må ta nye digitale hensyn for å kunne overholde kildevernet. De må beskytte seg på andre måter enn tidligere når nesten all kommunikasjonen foregår digitalt på Internett. Med datamaskiner, mobiltelefoner og nettbrett er journalisten tilknyttet Internett med mange medium. Teknologien åpner mange dører og gjør gravejournalistikk mye enklere dersom man har gode IT-ferdigheter. Teknologien kan

også brukes mot journalistene med vonde hensikter. Utenforstående aktører kan være ute etter å skade eller innhente informasjon som tilhører journalisten eller redaksjonen. Cyberkriminalitet har vokst i takt med spredningen av datamaskiner, programvare og teknisk infrastruktur (Gottschalk, 2011, s. 1).

Når det gjelder utvalget jeg har foretatt så er det basert på konkrete saker om dataangrep som jeg har funnet gjennom research på Internett. Journalistene jeg har intervjuet har alle lang erfaring, og flere av dem har også internasjonal bakgrunn. De har jobbet med journalistiske temaer som politikk, teknologi, sport og etterretning osv. Jeg har hatt fokus på datasikkerhet og kildevern i intervjuene. Utgangspunkt mitt er fra episoder som journalistene har opplevd hvor det tyder på at de har blitt utsatt for dataangrep. Svarene jeg har fått i intervjuene har vært varierende, og det er stor forskjell på hvor sterke indikasjoner journalistene har på at de faktisk har blitt utsatt for en kriminell handling. Det som til gjengjeld har vært overraskende er at de har gode IT-kunnskaper, og forstår trusselen med at de kommuniserer på Internett, og lagrer informasjon digitalt.

Etiske hensyn

Jeg informerte alle informantene om at de deltar i min masterstudie, og jeg møtte ikke på noen nevneverdige etiske problemstillinger i undersøkelsene mine. Det at man har blitt utsatt for dataangrep kan skade journalistens rykte, men ingen av informantene virket å ha problemer med å stå frem og fortelle om opplevelsene rundt kriminaliteten de kan ha blitt utsatt for. Før jeg gjorde intervjuene hadde jeg aldri snakket med informantene, og hadde dermed ingen relasjoner til dem. Jeg opplevde stor velvilje ettersom de mente dette er et tema som må belyses sterkere blant journalister. Et av de fremste etiske kravene for god forskningsetikk på slike premisser er ærlighet og åpenhet (Tjora, 2012, s. 40). Jeg har hele tiden prøvd å være bevisst på hvilke konsekvenser deltakelsen i studien kan ha for informantene. Det er derfor enkelte funn jeg har unnlatt å skrive om, selv om det kunne være interessant for min studie.

Casestudie

Journalister og dataangrep er et forskningsområde det i liten grad er forsket på både her til lands, og ellers i verden. ”Hvis det er dårlig med teori på feltet, kan case-studier være nyttig for å få en første innsikt” (Østbye, Knapstad, Helland og Larsen 2007, s. 103). Jeg

håper at denne forskningen kan være med på å utvide kunnskapsfeltet rundt datasikkerhet og kildevern for journalister. Det er jo svært vanskelig å kunne si at man har blitt utsatt for datakriminalitet. Det gjorde at jeg hadde få tilfeller å velge mellom som oppfylte mine kriterier for undersøkelsen. Da jeg skulle velge metode for forskingen ønsket jeg å få dybdeinformasjon, og da falt valget på kvalitativ forskning og casestudie. "Ordet case kommer fra latin *casus* og betyr tilfelle, og metoden brukes inngående for å studere ett eller noen få tilfeller" (Johannessen, Tufte & Kristoffersen 2006, s. 84).

Mine fellestrekket som kriterieutvalg for casestudiet var at journalistene mente at de hadde blitt utsatt for dataangrep. Her var mitt hovedformål å utvikle kunnskap om temaet dataangrep og journalistikk. Jeg oppnådde rikholdig informasjon om de ulike casene som jeg har fokusert på i studien gjennom kvalitative dybdeintervjuer. Ifølge Tjora (2012, s. 105) mener Kvale: "Som hovedregel kan vi si at man bruker dybdeintervjuer der man vil studere meninger, holdninger og erfaringer. Vi er med andre ord ute etter livsverdenen til informanten". Det var en stor fordel at jeg hadde prøvd ut spørsmålene på forhånd slik at sjansen for misforståelser ble minimert. Alle situasjonene journalistene hadde opplevd var forskjellige, noe som gjorde det umulig å sammenligne dem.

> Et viktig formål med case-studier er at de har et mer generelt siktemål enn mer beskrivende undersøkelser som også baserer seg på flere metoder. Følgelig kan case-studier knyttes til undersøkelsesopplegg som er spesielt rettet mot å oppnå kunnskap som peker ut over den enheten undersøkelsen fokuserer på (Thagaard, 2009, s. 210).

Som det fremgår i sitatet ovenfor er case-studier en metode for å gi generell kunnskap. Jeg ønsker å kunne belyse et fenomen som tilsynelatende er viktig for at fremtidens kildevern skal kunne overleve teknologien. For å kunne kartlegge dette passet det bra å bruke et eksplorerende forskningsdesign slik at man kan bli kjent med undersøkelsesobjektene og problemfeltet. "Den ene ytterligheten i kvalitative forskningsopplegg er eksplorerende studier hvor hensikten er å utforske et felt som det er lite kunnskap om fra før" (Thagaard, 2009, s. 16). Min kvalitative forskning har gitt meg et viktig grunnlag for innsikt og forståelse i forhold til problemstillingen. En svakhet med dette forskningsopplegget er at jeg ikke kan vektlegge utredelse og betydning i samme grad som i en kvantitativ metode.

Intervjuet er en av de mest utbredte kvalitative metodene som i prinsippet er basert på et subjekt-subjekt forhold mellom forsker og informant. En av konsekvensene med dette er at både forsker og informant påvirker forskningsprosessen. Den informasjonen som informanten er villig til å bidra med er knyttet til hvordan forskeren blir oppfattet (ibid.). Dette er et forskningsfelt som alle informantene viste interesse for. Jeg føler at de var åpne og ærlige slik at de kan være med på å belyse utfordringene til kildevernet i teknologisamfunnet. Det er umulig for meg å ikke påvirke forskningsprosessen, men jeg har forholdt meg til de etiske retningslinjene innenfor forskersamfunnet ved å utvise redelighet og nøyaktighet i presentasjonen av forskningslitteraturen.

Kvalitativ metode – Semistrukturerte intervju

Jeg har gjennomført intervjuer med fire norske journalister som mener å ha blitt utsatt for dataangrep. I tillegg har jeg snakket med to norske journalister med IT-utdanning som har spesialkompetanse innenfor fagfeltet. Journalistene har jeg funnet gjennom kildearbeid, kontaktnettverk og søk på Internett. Det har vært svært krevende å finne disse journalistene ettersom det ikke er mange som ønsker å stå frem med at de har blitt utsatt for dataangrep. Det er svært få saker om norske journalister som har blitt hacket eller utsatt for dataangrep som er publisert på Internett. En av grunnene til dette kan være uvitenhet fra journalistenes side, men det er jo ofte negativt for alle samfunnsborgere å bli utsatt for en slik kriminell handling. Jeg har brukt kontaktnettverket mitt i media til å finne journalistene. Det har i stor grad vært en komplisert undersøkelsesfase om et tema det snakkes lite om blant journalister.

Alle journalistene jeg tok kontakt med som hadde vært utsatt for dataangrep var positive til det jeg jobbet med, og ønsket å stille til intervju. De ble informert om hvordan jeg hadde funnet frem til handlingen de hadde blitt utsatt for, og formålet med forskningen jeg jobbet med. Det var ikke mange journalister å intervjue som oppfylte kriteriene til forskningen min, og jeg har derfor intervjuet alle journalistene som mener de kan ha blitt utsatt for datakriminalitet. Tilgjengeligheten var derfor et stort problem både når det gjelder litteratur og forskning på området. Det var en svært tidkrevende prosess å finne informantene, og sjansen for at jeg fikk innpass så jeg selv på som liten.

Derfor gjorde jeg mye forarbeid slik at jeg var godt forberedt da jeg tok kontakt på telefon, og jeg tror mye av dette er grunnen til at de ønsket å stille opp.

Jeg valgte å benytte meg av semistrukturerte intervju med en intervjuguide (Vedlegg 1) hvor temaene var definert på forhånd. Krumsvik (2013, s. 62) refererer til Kvale som definerer dette intervjuet slik: ”Et intervju som har til mål å innhente beskrivelser av den intervjuedes livsverden med henblikk på fortolkning av de beskrevne fenomenene”. Dermed hadde jeg mulighet til å følge opp momenter som ikke var på intervjuskjemaet Før intervjuprosessen lagde jeg en intervjuguide, og denne intervjuformen gav meg stor fleksibilitet siden det dukket opp mange overraskende innspill. ”Spesielt viktig er det i denne delen å utvikle en intervjuguide som er nær knytt til forskningsspørsmåla i studien” (Ibid.).

Jeg ønsket å gi journalistene god kontroll i situasjonen slik at de kunne respondere på en naturlig måte ved å høre godt etter hva de sa. Rekkefølgen på spørsmålene var ikke spesielt viktig så lenge alle informantene svarte på alle temaene. Under selve intervjuet er det viktig med aktiv lytting , det vil si at vi både gjennom væremåten og spørsmålene vi stiller understreker vår deltakelse i samtalesituasjonen (Østbye et al., 2007, s. 103). Jeg var derfor en aktiv lytter, og ettersom dette var noe informantene selv mente var viktig gikk samtalene av seg selv. Det beste ville vært om informantene kunne svare på de samme spørsmålene slik at det ble enklere å sammenligne svarene i analysen. De fikk prate ganske fritt under intervjuene, men det var jeg som styrte samtalen dersom den sporet av, og sørget for å få informasjon innenfor alle temaene i intervjuguiden. Intervjuene ble derfor en mellomting mellom et strukturert og et semistrukturert intervju, der jeg kom med oppfølgingsspørsmål underveis.

Jeg tok notater under intervjuene slik at jeg senere kunne stille spørsmål basert på opplysningene informantene hadde kommet med. Noen av intervjuene ble gjort på Skype, mens resten ble gjort på telefon. Alle intervjuene ble tatt opp slik at jeg kan dokumentere intervjuene med opptak. På denne måten vil intervjuene være tilgjengelig for etterbehandling. Som Tjora sier (2012, s. 140):

> Av praktiske og økonomiske grunner blir det av og til nødvendig å gjennomføre intervjuer via telefon. Vi mister da muligheten til å bruke kroppsspråk. (…) Dermed forsvinner noe av samtaleaspektet som det gode intervjuet er avhengig av.

Dette ble ikke noe stort problem, men jeg skulle helst ha gjort alle intervjuene ansikt til ansikt eller på Skype. Rett etter at jeg var ferdig med intervjuene skrev jeg de ned i sin helhet. Intervjuene ble transkribert ordrett, men jeg tok bort unødvendige lyder og repetisjoner. Jeg var ikke ute etter å tolke informantene, men å få frem faktainformasjon og deres meninger om temaet på spørsmålene. Dette var nødvendig for å få oversikt og orden på datamaterialet, men jeg prøvde hele tiden å gjengi det de hadde sagt slik at budskapet ikke endret mening. Man bør ha tilgang til det som ble sagt ettersom det er svært problematisk å nøye seg med det vi oppfattet ble sagt i intervjusituasjonen (Østbye et al., 2007, s. 103).

Til slutt kodet jeg intervjuene etter intervjuguidens oppbygning slik at materialet skulle bli oversiktlig. Dette var en forholdsvis enkel oppgave ettersom jeg hadde fulgt intervjuskjemaet ganske slavisk, kun oppstukket av enkelte oppfølgingsspørsmål. Enkelte ganger kom informantene også med opplysninger som passet inn under andre tema slik at jeg måtte flytte dem dit hvor de passet inn. I analysen har jeg vært svært opptatt av å finne likheter og motsetninger som jeg hadde i informasjonen. Det er de enkelte journalistenes opplevelser om datasikkerhet og kompetanse om kildevernet som har lagt grunnlaget for min egen analyse.

Jeg mener at reliabiliteten er ivaretatt på en god måte. Jeg har vært svært opptatt av at forskningen skal være gjennomført på en pålitelig og tillitsvekkende måte. ”Begrepet reliabilitet refererer i utgangspunktet til spørsmålet om en annen forsker som anvender de samme metodene ville kommet frem til samme resultat” (Thagaard, 2009, s. 16). Det er jo ikke enkelt å etterprøve et slikt studie så troverdigheten må ivaretas på en anstendig måte. Jeg har derfor redegjort grundig i dette metodekapittelet for hvordan dataene er blitt utviklet i løpet av forskningsprosessen. Om validiteten er ivaretatt avhenger i stor grad om man har undersøkt det som man hadde til hensikt å undersøke, noe jeg mener å ha gjort. Som Thagaard (2009, s. 209) sier: ”Vi kan presisere begrepet validitet ved å stille spørsmål om de tolkninger vi kommer frem til, er gyldige i forhold

til den virkeligheten vi har studert". Jeg har gått kritisk gjennom analyseprosessen, og samtidig gitt gode begrunnelser for undersøkelsens konklusjoner.

Kapittel 6 – Analyse av den kvalitative undersøkelsen

Dataangrep

Et sentralt spørsmål til journalistene er om de har blitt utsatt for dataangrep. Dette er det nesten umulig å svare ja på ettersom det er svært vanskelig å dokumentere. Det vil dermed bli mer en fortelling fra journalisten sitt ståsted om hva de har opplevd som kan antyde om datakriminalitet har funnet sted. Verken jeg eller journalistene kan være sikre på at hacking eller overvåkningen har funnet sted. Som Espen Andersen fra NRK sier: "En vellykket hacking gjøres jo skjult slik at man ikke er klar over det selv. Jeg trur ikke jeg har blitt hacket, men man kan aldri vite dette." Jeg vil med dette som utgangspunkt fortelle historiene deres. Et sentralt spørsmål til journalistene er derfor om de har blitt hacket? Anders Brenna har jobbet som journalist med IT som fagfelt, og har følgende å fortelle:

> Jeg har ikke blitt hacket som jeg vet om, men jeg antar at det har skjedd noen ganger. Jeg kan derimot ikke si noe om verken tidspunkt eller hvordan. (…) Jeg vil tro og anta det uten at jeg har noen som helst bevis for det. Når jeg holdt på med "Stopp Datalagringsdirektivet" så ble jeg sjekket ut både på telefon og e-post. Det hadde jeg selv gjort hvis jeg jobbet i PST for å si det sånn (Brenna).

Dette blir bare spekulasjoner fra Brenna sin side, men han har jobbet lenge i IT-bransjen, og skrevet boken *Digital kildevern* om digitalt kildevern, så dette er et fagområde han kjenner godt til. Det er derfor med god teknisk innsikt og forståelse av hva datasikkerhet handler om at han kan uttaler seg på denne måten. Han har derimot ingen direkte indikasjoner på at hacking har funnet sted, men har god forståelse av hva som kjennetegner en vellykket hacking.

> Det som er hele poenget med et hackerangrep er jo nettopp at det kjennetegnes ved at ingen vet om det. Fordi at i det øyeblikket du vet om et hackerangrep så gjør man alle mulige tiltak. Hele essensen i et hackerangrep er at det kjennetegnes ved at ingen vet om det, eller skal merke at de har vært der for da

> kan man sitte og lytte gang etter gang. Da er det ingen som tar noen tiltak i ettertid for å gjøre noe med det. Hele essensen er å ikke legge igjen spor om at man har hacket for da kan man gjenta det uten at mottiltak blir gjort i ettertid (Brenna).

Av de journalistene jeg har snakket med er nok Anders Brenna en av de som har best IT-ferdigheter, men han er kanskje mest kjent for å være en av de største motstanderne av Datalagringsdirektivet, heretter kalt DLD. Brenna sier at man skal ikke gjøre andre journalister paranoide slik at de ikke ønsker å kommunisere ved hjelp av digitale verktøy. Likevel må man må være bevisst på faren man utsetter kildene sine for. Et vellykket hackerangrep er at man har brutt seg inn på en datamaskin eller server uten at brukeren av denne har oppdaget noe som helst. Da kan man gjenta ugjerningen gang på gang slik at man har full kontroll på hva vedkommende holder på med.

Etter at Aftenposten publiserte Wikileaks-dokumentene i en rekke artikler i januar 2011 så ble nyhetsredaktøren Ole Erik Almlid utsatt for hackerangrep. Almlid kan ikke utelukke at hackerangrepet hadde sammenheng med avisens Wikileaks-dekning (TV 2, 06.11.2011). Disse avsløringene skapte enorm interesse verden over, men krevde også at de som publiserte dette sensitive materialet hadde stort fokus på datasikkerhet. Etter å ha fått tilgang til 250.000 Wikileaks-dokumenter kunne Aftenposten bruke dokumentene uten betingelser, men de oppga aldri hvem som var kilden. Etter at Almlid selv hadde skrevet artikler basert på Wikileaks materialet ble han utsatt for dataangrep.

> Jo, det var slik at på morgenen når jeg sto opp så bruker jeg alltid å sjekke mailen min, for å se om det er noe viktig jeg må besvare. Akkurat i tidene med Wikileaks-publiseringene så hadde jeg veldig mye mailer hele tiden, og intervjuforespørsler fra hele verden. Jeg fikk da en intervjuforespørsel fra en japansk allmennkringkaster. De ønsket å komme til Norge å intervjue meg osv. E-mailen så jo veldig ordentlig ut, og inneholdt en intervjuforespørsel, tidspunkt og alt mulig annet. Når jeg kom på jobb og slo på maskinen min så begynte den å synkronisere seg med en gang, mobilen begynte samtidig å synkronisere. Jeg har opplevd masse forskjellig, men ikke noe sånt. Ikke noe liknende som det der (Almlid).

Aftenposten sier at de var ekstra forsiktige og økte datasikkerheten før og under publiseringen av Wikileaks-dokumentene, så det som skjedde med Almlid var ingen stor sak for avisen (ibid.). De har ingen anelse om hvem som står bak dataangrepet eller hva som egentlig skjedde. IT-arbeiderne i Aftenposten prøvde å finne gjerningsmennene,

men det er svært krevende å følge slike spor. Dette gjør at Aftenposten må leve med uvissheten om hva som egentlig skjedde, og de må da stole på at aktøren som ønsket å hacke dem ikke fikk noe utbytte av dataangrepet. De vil aldri få svar på hva som var intensjonen med angrepet, og kan derfor ikke være sikre på om aktøren kun gjorde dette ene forsøket på datainnbrudd, eller om de har jobbet skjult på innsiden av Aftenposten sine servere over lengre tid. At det var et hackerangrep har IT-arbeiderne konkludert med, noe jeg kommer tilbake til. Å komme seg inn på IT-systemer gjennom e-post er en kjent metode som brukes mye for å utnytte sikkerhetshull. Det er slik at et overvåkingsprogram installeres dersom man for eksempel åpner et vedlegg. Om det var dette som skjedde med Almlid er usikkert.

En journalist som har jobbet tett opp mot hackermiljøet både nasjonalt og internasjonalt er Kjetil Stormark. Han fikk kontakt med Anonymus i 2011 da diskusjonen rundt DLD herjet som verst. Grupperingen Anonymus er en gruppe løst sammenknyttede individer fra hele verden. De har ikke noen ledelse, og de tar tak i saker dersom mange nok anser det som riktig. Uten noen klar visjon er de snarere anonyme hackere som gjør det som måtte falle dem inn (Hardware 30.12.2010). Stormark hadde kontakt med hackerne i samme periode som hjemmesiden til Arbeiderpartiet ble utsatt for et tjenestenektangrep med DDOS-metoden. Serveren kollapset etter at hackere sendte enorme mengder data til nettserveren for hjemmesiden på samme tidspunkt. Dermed kollapset serveren etter å ha blitt utsatt for 4000 forespørsler i sekundet. Fem unge menn ble senere dømt for hackerangrepet, og det var gruppen Anonymus som kort tid etter innrømmet ugjerningen. De mente innføringen av DLD var et angrep på deres og andre nordmenns privatliv (NRK, 02.04.2014). Stormark har derfor en unik erfaring om hva disse menneskene kan være i stand til å gjøre etter å ha fulgt dem svært tett i flere måneder.

> Allerede da jeg begynte å følge hackermiljøet skjønte jeg instinktivt at dette kom til å bli risikabelt. Jeg oppjusterte derfor min IT-sikkerhet en god del. Jeg har jobbet med etterretning som tematikk siden midten av 1990-tallet. Jeg har tidligere opplevd at langt mer avanserte aktører enn hackere, altså enkeltpersoner, har forsøkt å gå etter kildene mine. Jeg opplevde blant annet dette i 2002/03, der det trolig var amerikansk etterretning som prøvde å krysspeile hva jeg arbeidet med. Årsaken var trolig at jeg kom tett innpå flere allierte etterretningsoperasjoner, der minst en hadde som hovedformål å forsøke å lokalisere hvor Osama Bin Laden oppholdt seg, sør i Afghanistan. (…) Det tok

> ikke veldig lang tid fra jeg etablerte kontakt med noen av de proffeste hackerne på verdensbasis før jeg begynte å oppleve alvorlige driftsproblemer på mitt eget datanettverk (Stormark).

Dette kan være en indikator på at noe er galt, og Stormark virker å ha gode IT-ferdigheter. Han forstår også viktigheten med datasikkerhet når han forteller sin historie. Flere av de andre journalistene har navngitt Stormark som en journalist de kan stole på når det gjelder kildevern og datasikkerhet. Det som skiller dette dataangrepet fra de andre er at Stormark fikk tydelige driftsproblemer med datamaskinen. Dette trenger ikke å bety at det har vært noe hackerangrep, men med tanke på kunnskapen og erfaringen vedkommende besitter så kan man ikke se bort fra at et hackerangrep fant sted.

Kristoffer Rønneberg jobbet en periode som stringer for Aftenposten i Beijing og opplevde overvåkning tett på kroppen ved flere anledninger. Han sier at det er et samfunn som bruker enorme ressurser på sikkerhet, og på å forhindre at gal type informasjon kommer ut. ”Hvis jeg var ute på reportasje og snakket med folk jeg ikke skulle, eller befant meg på steder som ble regnet som sensitive, kom det med en gang folk å spurte hvem jeg var, og hva jeg skulle og ville vite navnet mitt” (Rønneberg). Så de som jobbet som utenlandske journalister i Beijing synes det var utrolig merkelig om de ikke ble overvåket.

> Det er vanskelig å si at "Ja" vi ble overvåket (…). Vi som var utenlandske journalister der nede snakket mye om overvåking og tok det for gitt at vi ble utsatt for dette. Jeg har ikke noen håndfaste bevis på at det skjedde, men det ville være veldig rart om det ikke skjedde ettersom vi var få utenlandske journalister i Bejing på den tiden (…). Vi hadde mobiltelefoner, men det var også mye av telefonsamtalene som foregikk på fasttelefoner. Internett var så tregt at det tok vi for gitt at det var "buget" (Rønneberg).

Det som skiller Rønneberg fra resten er at han har jobbet i et journalistisk landskap hvor myndighetene er kjente for å kontrollere pressen. I 2011 sendte kommunistpartiet ut forskrifter til pressen der mediene fikk beskjed om å tone ned kontroversielle saker for fordelaktig dekning av partiet. Organisasjonen Reportere uten grenser sier at de er sjokkerte over det de mener viser nivået på kommunistpartiets forsøk på å kontrollere informasjon og innføre sensur i landet (TV 2, 21.01.2011). Dette betyr ikke at Rønneberg

ble digitalt overvåket, men holdningen myndighetene har til journalistene skiller seg radikalt fra det vi opplever her i Norge, og dette fikk Rønneberg oppleve.

Angrepet og mulige bakmenn

For å kunne forstå bedre hvordan journalistene oppdaget selve dataangrepet kommer jeg til å gå mer i dybden på hva de mener kan ha skjedd. I denne delen kommer jeg også til å gå nærmere inn på hvem som kan stå bak dataangrepet på journalistene. Dette blir igjen spekulasjoner ettersom man ikke har kunnet dokumentere dataangrepene. Her må man bruke sunn fornuft, og IT-ferdigheter for å kunne sette seg inn i situasjonen som journalistene har opplevd. Anders Brenna er mest kjent som lederen i organisasjonen Stopp Datalagringsdirektivet. Han har sterke mistanker om at han ble overvåket da han var talerør for motstanderne av DLD. Motstanden mot direktivet var stor, og Brenna var svært engasjert i å prøve å forhindre at DLD skulle bli vedtatt.

> Gitt at PST sa at de sjekket sakene med Anonymus så ville det vært rart om de ikke overvåket meg også. Dermed er spørsmålet om jeg da var aktivist for Stopp Datalagringsdirektivet, eller en frilansjournalist, noe som jeg var på den tiden. Så jeg ville si at det ville vært logisk av dem å sjekke meg ut på det tidspunktet, og sjekke telefon og e-post dersom de hadde muligheten til det, men jeg kan ikke dokumentere at de har gjort det (Brenna).

Ettersom det ble spekulert i om Brenna var en del av Anonymus på den tiden så kan man ikke se bort fra at han var en av dem som ble sjekket opp av PST. Etter at Anonymus-hackerne ble overvåket av PST gikk de berserk. Norske journalister tok derfor kontakt med Brenna og trodde han var en del av dette nettverket. "Du som er med i Anonymus! Jeg svarte kontant at jeg ikke er med der. Jeg overholder kildevernet så du kan si det til meg" (Brenna). Journalistene fortalte Brenna at de overholdt kildevernet, og de som kontaktet han tok for gitt at han var en del av Anonymus. Brenna svarte følgende:

> Vet du hvem som er nødt til å jobbe overtid og sitte oppe hele natten for å sikre serverne osv. hvis Anonymus hacker. Det er ikke politikerne de angriper det er IT-folk sånn som meg som må fikse opp i problemene. Da begynte det å gå opp for dem at jeg ikke er med på den type ting (Brenna).

Rønneberg var journalist i Kina da Google ble hacket (Dagbladet, 19.01.2010). Han husker selv at det var andre journalister som ble overvåket i Kina på den tiden.

Rønneberg ble anbefalt av andre journalister å bytte passord på sin Google-konto etter å ha vært en del av en liste med deltakere som fikk overvåket sine e-post kontoer.

> Det var flere akademikere og journalister som opplevde å bli overvåket. De fortalte meg at navnet mitt var på en kontaktliste i e-posten deres som hadde blitt hacket. Det var noen som hadde lagt inn en mailadresse som gjorde at alle e-postene vi sendte ble videresendt til en ukjent mottaker (Rønneberg).

Spørsmålet er hvem denne mottakeren var og hva vedkommende skulle med informasjonen til disse journalistene? Han er helt sikker på hvem som kan ha stått bak overvåkningen: "De kinesiske myndigheter, altså sikkerhetsbyrået i det kinesiske kommunistpartiet". Rønneberg har opplevd at det var problemer med kommunikasjonen mens han jobbet som journalist i Kina. "Jeg har selv opplevd at mailer som jeg skulle motta eller sende ble borte på mystisk vis mens jeg bodde i Kina". Dette er tydelige indikasjoner på at han kan ha blitt overvåket. Det var ansatte i Google i Kina som ble mistenkt for å ha stått bak overvåkningen og de 700 ansatte i selskapet mistet tilgangen til det interne nettverk da etterforskningen pågikk (Ibid.). Som følge av dette har også Google vurdert å trekke seg ut fra det kinesiske markedet på grunn av kinesiske krav om sensurering av Internett. Det var bare tilfeldigheter som gjorde at Rønneberg fikk vite at han var på listen over personer som kan ha blitt overvåket. Hva annet som kan ha skjedd kan man bare spekulere på.

Som Almlid tidligere var inne på, oppdaget han at mobiltelefonen og datamaskinen begynte å oppføre seg merkelig. Ettersom han da var oppmerksom kan det se ut som han klarte å avverge dataangrepet han ble utsatt for. Det er vanskelig å si hva slags type dataangrep dette var, men det kunne nok fått større konsekvenser enn det fikk dersom han bare hadde oversett at datamaskinen og mobiltelefonen oppførte seg merkelig. Han husker godt hva som skjedde og virker å ha god forståelse og respekt for at noen var interessert i informasjon hans.

> Jeg husker at mailadressen var litt rar. Den var lik den japanske tv-kanalen, men ikke helt lik. Og når jeg så det, så bare rev jeg ut kablene til Internett og kastet meg over maskinen, og slo av og rev ut noen kabler og sånt, for da skjønte jeg at det måtte være noe galt. Da jeg senere slo på maskinen virket den normalt, og da ble det undersøkt om noe suspekt hadde skjedd. Vi skjønte da at det var et avansert form for dataangrep. Hvis jeg ikke hadde gjort noe mer med det så ville

> det aldri blitt oppdaget, for da hadde den stått og sendt informasjon som jeg har hentet fra min maskin via mail, uten at jeg hadde merket det. Det var hele greia (Almlid).

Det er et viktig poeng Almlid har om at hvis han ikke hadde foretatt seg noe når mistanken var der så hadde datakriminaliteten aldri blitt oppdaget. Å oppdage et dataangrep kan være ekstremt krevende, og denne gangen endret det tekniske utstyret sine vaner slik at Almlid var påpasselig, og fikk koblet datamaskinen av Internett. Hva som ble synkronisert kan man jo spekulere i uten å bli klokere av den grunn, og det kunne jo ha vært en normal synkronisering som gjorde at Almlid ble paranoid. De satt på mye sensitiv informasjon fra Wikileaks som mange utenforstående kunne være interessert i å få tak i. Dette kan være grunnen til at de opplevde mye aktivitet på den tiden. Hva de eventuelt fikk ut av angrepet er derfor uklart, men det er utvilsomt sterke indikasjoner og en kjent fremgangsmåte å hacke noen på.

Stormark opplevde store driftsproblemer mens han jobbet med hackermiljøet og fikk tips fra dem om hvordan han kunne sikre seg. Hackerne i Anonymus var ekstremt opptatte av anonymitet og at kildevernet ble opprettholdt. De instruerte derfor Stormark om hvordan han kunne øke egen datasikkerhet slik at det ble tryggere for dem å kommunisere med hverandre. De brukte programvaren Skype og mIRC til å kommunisere med hverandre på etter at hackere hadde fortalt at dette var de sikreste kommunikasjonskanalene på Internett.

> Jeg hadde i den perioden unormalt mye heng på maskinen. Jeg har verken før eller siden hatt så mye IT-problemer. Jeg fulgte nøye med på prosessoraktiviteten. Dersom det ble startet prosesser på maskinen som jeg selv ikke hadde initiert, brøt jeg som regel bare nettforbindelsen (Stormark).

Det er ikke mange PC-brukere som går inn og sjekker prosessoraktiviteten. Ved å sjekke prosessoraktiviteten kan man se hvilke prosesser som kjøres på datamaskinen for å se hva den bruker kapasiteten sin på. De færreste av oss har IT-kompetanse til å forstå hva de forskjellige prosessene er, så her må det litt IT-kunnskaper til for å forstå hva som egentlig skjer. Dersom det startes prosesser som man ikke kjenner til er dette muligens programmer som startes av andre som forsøker å komme seg inn på din datamaskin. Hackere er jo klar over at de gjør noe ulovlig, og er derfor redde for å bli avslørt. De

kunne jo heller ikke stole på at Stormark var den han utga seg for å være. Etter hvert som han fikk opparbeidet tillitsforholdet til de norske hackerne så åpnet det opp nye dører slik at han kom i kontakt med hackeativister i mange andre land. Han kom blant annet i kontakt med hackergruppen LulzSec.

> Det var da jeg opprettet kontakt med LulzSec at jeg opplevde en del uregelmessigheter. LulzSec var hackergenerasjonens ukontrollerbare cowboyer. De hadde angrepet både NSA, CIA og NATO. Jeg tror ikke de var redde for å angripe en journalist. Jeg kan si med sikkerhet at det var de som stod bak, men det var i hvert fall et påfallende sammenfall i tid (Stormark)

Som Stormark sier så er det jo påfallende at dette kan ha vært et hackerangrep fra LulzSec. Man får fort inntrykket av at han har gode IT-ferdigheter og tar datasikkerheten på alvor når han prater om dataangrepet. Dette er et inntrykk både jeg og andre journalister jeg har intervjuet sitter igjen med. Han bruker tekniske ord og utrykk som man må ha gode IT-kunnskaper for å forstå, samtidig som man hører at han tar mange forholdsregler for å beskytte informasjonen sin fra andre. LulzSec har gjort langt værre ting enn å hacke en norsk journalist, og angrepet større aktører med mye mer avansert datasikkerhet. Det burde vært et enkelt bytte for dem å skade eller sabotere utstyret til Stormark med tanke på andre ugjerninger de har gjort, og spørsmålet er derfor hvor mye ressurser de ønsket å bruke på vedkommende. Stormark har også kryptert informasjonen på sine datamaskiner. Det er derfor svært krevende å knekke kryptoalgoritmen slik at informasjonen på datamaskinen blir forståelig. En av hackerne i LulzSec som ble avslørt gikk med på å bli informant for FBI mot å få redusert straff, noe som blant annet bekreftes av BBC (Digi 07.03.2012). Stormark sier følgende om den saken: ”I forlengelsen av det kan man jo diskutere hvem som egentlig ledet arbeidet med angrepene?”.

Poenget med alle disse sakene er at ingen av dem kan være 100% sikre på at et dataangrep har funnet sted. Når man derimot hører om hva de har opplevd i de enkelte tilfellene, er det åpenlyst at det har foregått aktivitet som de har opplevd som en trussel utenfra. Dette er tydelig journalister som har bra fokus på datasikkerhet og forstår alvoret med digitalt kildevern. Nesten all informasjon lagres i dag digitalt med Internett som kommunikasjonsplattform, noe som lar informasjonen være tilgjengelig over hele verden.

Tanker om det som skjedde og hensikter?

Rønneberg opplevde stadig å bli overvåket ved at noen fulgte etter han, noe som er et kjent problem for utenlandske journalister som jobber i Kina. Dette betyr ikke nødvendigvis at han ble overvåket på andre måter enn at noen spanet på han. Dette var en del av hverdagen, og han opplevde flere ganger å bli kastet ut fra steder han befant seg.

> Jeg er jo klar over at de fulgte med på hva jeg gjorde, og at ambassaden i Oslo fulgte med på alt jeg skrev. Hver gang jeg snakket med ambassaden eller UD kunne de referere til saker jeg hadde skrevet om, og ting de ville utfordre meg på da. Dette skjedde spesielt på slutten av året ettersom man får fornyet arbeidstillatelse en gang i året (Rønneberg).

Som følge av dette måtte Rønneberg møte til intervju med UD for å diskutere jobben han gjorde i Kina. Det er først og fremst journalister som UD er usikre på som blir innkalt til denne *te-koppen* som Rønneberg selv kaller det. De gjennomgikk da en del av sakene hans, og mente han var for kritisk og for lite objektiv, samtidig som han brukte feil type kilder.

> Kina er et diktatur og de er veldig opptatte av å styre budskapet slik at det er deres versjon av sannheten som folket får høre. De er livredde for et opprør. De kinesiske journalistene har de veldig god kontroll på ettersom de er underlagt det kinesiske propaganda byrået alle sammen (Rønneberg).

Kinas kommunistmyndigheter setter alle journalister på skolebenken for å lære dem om et mer marxistisk styresett. Flere hundre journalister, bloggere og advokater har blitt arrestert som følge av "ryktespredning og for å provosere frem bråk". Det er ikke enkelt for befolkningen i Kina å forholde seg til det som publiseres i et land hvor pressen ikke får lov til å skrive det som er sant. Hvordan skal folket kunne sjekke hva som er rett og galt når alle medier i Kina er kontrollert og sensurert av kommunistpartiet, og det enorme maktapparatet?

> Det var mye verre med oss utlendinger som kom dit med et helt annet perspektiv og forståelse av det meste. Dette førte til at det ble kulturkrasj, og de har helt andre formeninger om hva journalistikk er for noe. Jeg vil ikke si at de prøvde å sensurere, men de prøvde i større grad å påvirke, med liten kunnskap eller forståelse om hvilken verden vi kom fra (Rønneberg).

Da Almlid forstod at han hadde blitt utsatt for et dataangrep, begynte IT-folkene i Aftenposten å etterforske angrepet og prøve å finne ut hvem som kunne stå bak kriminaliteten. Datamaskinen til Almlid ble skrotet etter hendelsen. Han mener Aftenposten var forberedt på at utenforstående kunne begå slike handlinger etter Wikileaks-publiseringene, og kilden som ga Aftenposten eksklusiv tilgang til alle dokumentene, er fortsatt anonym.

> Vi hadde jo tatt viktige forholdsregler i forhold til eventuelle dataangrep. Selv om maskinen min hadde blitt infisert eller ødelagt av angrepet, og jeg ikke hadde merket noe, så ville det aldri ha skjedd at de hentet ut Wikileaks-dokumentene, for de lå på lukket server (Almlid)

Man kan aldri sikre seg godt nok, men så lenge serveren ikke var tilknyttet Internett må man komme seg innenfor Aftenpostens lokaler for å kunne få tak i informasjonen som ligger lagret der. Aftenposten forstod selvsagt at Wikileaks-materialet var av stor internasjonal interesse, og det fantes store politiske interesser som ønsket å finne kildene bak disse lekkasjene.

> Ja, dem mente at enten måtte det være en nasjon med store midler eller et multinasjonalt selskap som ble sporet tilbake til Singapore. Unntatt at det trenger å bety noe som helst, men IT-folkene tror det var et veldig dyrt angrep, og de som gjorde det måtte ha hatt mye penger (Almlid)

Det er mulig å spore enkelte dataangrep til lokaliseringen hvor angrepet fant sted, men det å finne ut hvem som stod bak handlingen er langt vanskeligere. Dersom man finner IP-adressen kan man også finne ut hvor i verden angrepet kommer fra, men også her kan man bli lurt ettersom det finnes programvare som kan manipulere datamaskinens IP-adresse, slik at det ser ut som man er andre steder enn der man faktisk befinner seg. To måter å gjøre seg litt mer anonym på er å la nett-trafikken gå via en mellomtjener eller proxyserver (ofte kun kalt proxy). Den andre er å bruke et VPN – virtuelt privat nettverk. Denne metoden brukes ofte dersom man ønsker å benytte seg av tjenester på Internett som er rettighetsbundet til enkelte land, som for eksempel norsk nett-TV fra utlandet (Hardware, 12.11.2012).

Noe nettinnhold er eksklusivt for visse geografiske soner, noe man legger merke til når det gjelder for eksempel musikk eller TV. Dersom man har store ressurser kan alle angrep spores, men det er ofte svært krevende ettersom motparten ofte har god beskyttelse, og bruker metoder som er manipulerende samt sikrer vedkommende mot å bli avslørt. At Almlid ble forsøkt hacket er ganske tydelig, men *hvorfor* får man aldri svar på. Han mener selv følgende om hvorfor de kunne være ute etter akkurat han: "Fordi jeg var den journalisten som hadde uttalt seg på vegne av Aftenposten, og det var jeg som var talsperson for saken. Og de antok vel at jeg hadde tilgang på Wikileaks-dokumentene gjennom min PC" (Almlid).

Brenna som ble koblet opp mot Anonymus etter hackerangrepene som ble satt i gang etter vedtaket om å innføre DLD, sier følgende om hvorfor han kan ha blitt hacket. "Hvis de var ute etter noe så er det jo kommunikasjonen mellom meg og Anonymus samt andre mistenkte. Noen av de tiltakene som ble gjort av PST var jo i beste fall i grenselandet mellom ulovlig eller ikke" (Brenna). Det har skjedd at norske hackere har blitt dømt for "Denial of service"-angrep tidligere, men det kan også ha vært andre som prøvde å hacke seg inn. Etter at DLD ble vedtatt i Stortinget fikk politikere fra Høyre og Arbeiderpartiet fylt opp e-postkassene sine med sjikane. De ble hetset og truet etter at DLD ble vedtatt. Med meldinger som "Vi vet hvor du bor", "Din jævel", og "Dette skal dere få svi for" (VG, 06.04.2011). Brenna sier: "Det var jo også noen som kom med trusler mot politikere, og dette er jo noe man bør akseptere for å si det sånn". Dette er en vanlig reaksjon fra hackerne som ønsker hevn, men som Brenna sier burde de selvsagt akseptere avgjørelsen uten å stikke kjepper i hjulene til politikerne ved å komme med trusler etter vedtaket.

Espen Andersen fra NRK som har lang erfaring med IT-sikkerhet har uttalt at man aldri kan være sikre på at man har blitt utsatt for hackerangrep. Han sier følgende om hvorfor akkurat han kunne være et interessant objekt for hackere.

> Hvis jeg skal snakke på vegne av meg selv, må der være folk som er ute etter dokumentasjon som vår redaksjon er i besittelse av. I tillegg må det være kildesensitivt materiale, altså informasjon fra kilder som skal ha beskyttelse, men som noen kanskje ønsker å utnevne her. En annen grunn kan være for å få tak i data. Vi håndterer jo også sensitive data som for eksempel skattelistene. Vi har

> også en del dokumenter etter samarbeidet med Wikileaks som også kan være potensielle sensitive dokumenter som kan lekkes (Andersen).

Dette viser tydelig at datasikkerhet må tas på alvor ettersom det aller meste av informasjon blir lagret digitalt. Dersom dataene ligger på en enhet som er tilknyttet Internett er de altså mulig å nå fra hele verden. Det er måten man beskytter informasjonen på som avgjør hvor utilgjengelig informasjonen skal være. Med sunn fornuft og fokus på å sikre sine data skal det lite til for å gjøre at den blir vanskeligere å nå for folk flest. Det finnes midlertidig mennesker der ute med ekstreme IT-ferdigheter som uansett vil være kapable til å kunne få tak i denne informasjonen dersom den er interessant nok for vedkommende. "Det er ikke i tvil om at dette er en reell fare så det er viktig at man er oppmerksomme og tar forholdsregler" (Andersen).

Stormark sier han er ganske sikker på at han hadde god nok datasikkerhet til at hackerne ikke fikk tak i sensitiv informasjon som han satt på i forbindelse med kontakten han hadde da han jobbet med Anonymus. Når man opplever hendelser utenom det vanlige på sine teknologiske medier, samtidig som man sitter på sensitiv informasjon, er det ikke usannsynlig at man blir paranoid. Gjennom media får man ofte høre om diverse overvåkningsskandaler, og andre ugjerninger som har oppstått etter dataangrep. Stormark sier at han måtte overbevise mange av hackerne han kom i kontakt med om at han ikke var fra FBI, men jobbet som journalist. Hackerne selv er klar over at det de holder på med er straffbart, og at de blir jaktet på.

> Jeg kan jo vanskelig bedrede dem for hackingen, og for at de forsøkte å finne ut hva jeg drev med. Paranoiaen på nettet er ganske ekstrem. Jeg opplevde flere ganger da jeg logget på IRC-kanaler, at folk ble helt hysteriske da jeg sa jeg var journalist. De var overbevist om at jeg var fra FBI (Stormark).

Hvem kan ha interesse av hacke en journalist

Det kan være mange grunner til at man ønsker å hacke en journalist. Enten det er for å skremme journalisten med trusler, sabotere, stjele eller overvåke. Dette varierer etter hva som er hensikten med ugjerningen. Det er nok mange journalister der ute som spør seg selv, hvorfor skulle noen ha interesse av å hacke meg? Noen er selvfølgelig mer aktuelle ofre enn andre, avhengig av hvilket stoffområde de jobber med, og verden er

ikke slik at noen har intensjon om å hacke alle journalistene. Jeg har derfor spurt journalistene om hvem som kan være interessert i å hacke dem? De kommer med flere eksempler på situasjoner hvor de kan være utsette. Hvis man tenker på at IT-eksperter er sikre på at Kina stod bak angrepene mot New York times, og at nasjoner velger seg denne typen mål har Stormark følgende oppfatning: ”Når ulike nasjoner velger seg denne typen mål, må ingen forsøke å overbevise meg at man har større respekt for journalisters integritet”.

Stormark sier at det avhenger av hva journalisten jobber med. Dersom en person for eksempel jobber med olje/gass som stoffområde, kan det være mange som har interessere av å følge med på journalistens virksomhet. Det kan være motivert ut i fra industrihemmeligheter, men kanskje spesielt jakten på børssensitiv informasjon.

> Å ha informasjon om en børssensitiv avsløring som kan drive kursen opp eller ned, kan ha vanvittig stor verdi hvis man sitter med denne kunnskapen ett eller flere døgn før alle andre. Kina kan eksempelvis være interessert i både bedriftshemmeligheter men også forhold som truer deres politiske interesser (Stormark).

Aftenposten-journalisten Rønneberg mener at det alltid finnes noen som ønsker å påvirke journalistikken din, og ønsker å vite hva du holdet på med. Han mener at faren for dataangrep ikke er grunn nok til at journalisten skal være paranoid eller forsiktig. Dersom man jobber med norsk militærindustri er det snakk om store verdier. ”Da er det helt sikkert interesser på den andre siden som ønsker å sette deg på et annet spor enn det du er inne på. Dette er jo en helt annen liga enn hva de har i Kina", sier Rønneberg. Dette fikk vi bevist i 2013 da Forsvarets etterretningsbataljon drev ulovlig kartlegging av blant annet to VG-journalister. Etter å ha jobbet med kritisk journalistikk om de hemmelige tjenestene i landet i en årrekke ble de kartlagt av PST. Leder for EOS-utvalget Eldbjørg Løwer sier at det gjaldt registreringer av personopplysninger. Sjefsredaktør i VG Torry Pedersen tror kartleggingen har skjedd fordi de to har skrevet flere oppsiktsvekkende saker med tilknytning til etterretning. Pedersen mener likevel det er helt uakseptabelt at Forsvaret bruker sine ressurser på å kartlegge nordmenn (TV 2, 21.03.2013).

Anders Brenna forteller om såkalte ”Information brokers”- miljøer som får tak i informasjon og selger den til andre kriminelle. Dersom dette er tilfelle mener han at det vil være naturlig å gå etter journalister som er et nav i samfunnet. De kan vite hvem som snakker med hvem, samtidig som de besitter mye sensitiv informasjon. ”Det er jo utrolig hva du som journalist får tak i av informasjon så lenge man sier de magiske ordene og holder ord. For da vet profesjonelle kilder at da er karrieren til journalisten over hvis han ikke holder ord” (Brenna). Uansett om det er myndigheter eller private interesser som er interessert i å hacke en journalist er det liten tvil om at sensitiv informasjon vil være attraktivt for svært mange som opplever å få sin sak satt på dagsorden også i fremtiden.

Datasikkerhet

Man har nå fått ett innblikk i hvorfor journalistene ovenfor mener å ha blitt utsatt for dataangrep. Det er ingen av angrepene som er dokumentet, og bakmennene er fortsatt ukjente. Man får fort et inntrykk av at dette er journalister som forstår faren ved å ta digitalt kildevern på alvor. De bruker også et teknisk språk hvor man får et inntrykk av at de har gode IT-ferdigheter. Hvor mye det blir brukt i praksis og hvor god sikkerheten er kommer jeg nærmere inn på i denne delen. Man har kommet langt dersom man forstår at det ikke skal enorme IT-kunnskaper til for å få tak i dataene du selv tror ligger trygt lagret. Brenna som blant annet har jobbet for Aftenposten og Teknisk ukeblad, sier han ikke forstod alvoret med digitalt kildevern i perioden han var journalist.

> Det var jeg på ingen måte. Jeg var ikke flink til å beskytte meg selv og så enkelt er det. Man snakker med både den ene og den andre og tar for eksempel for gitt at noen kan ha interesse av å hacke seg inn på e-posten min, så da satser man heller på at det ikke ligger viktig informasjon der (Brenna).

Dette er altså en journalist som i tillegg har IT-utdanning, og som i dag jobber som forretningsutvikler i digitalselskapet Knowit. Han forstod etter hvert alvoret med digitalt kildevern, og har gjort en rekke tiltak for å prøve å holde kildene anonyme. ”På mine mest paranoide øyeblikk så har jeg sendt e-poster hit og dit. Nettopp for at man ikke skal kunne dokumentere at dette er en e-post som er sendt via en sånn tjeneste at hvis den er lekket så vet jeg at noen har vært inne på det. Dette er holdningen” (Brenna). Dette er en måte å prøve å avlede eventuelle kildejegere på. Han

tar dermed viktige forhåndsregler, og dette er verken tidkrevende eller vanskelig å få til for andre journalister som også jobber med sensitivt materiale.

> Hvor paranoid skal man være er jo også et spørsmål. En journalist er nødt til å snakke med andre ved hjelp av telefonen. Man kan ikke bli så paranoid at man ikke tør å bruke telefonen heller. Vi må prate, men vi må være klar over at det vi sier kan spores, og da bør man benytte alternative kommunikasjonsmetoder. Enkelte ting prater man ikke om på telefonen i det hele tatt (Brenna).

Journalistrollen handler mye om å kommunisere med andre så det er klart man må finne en balansegang. Enkelte saker er jo helt klart viktigere enn andre slik at her må man følge mageføelsen, og ikke glemme bort at det som blir sagt kan avlyttes eller spores i ettertid. Brenna er skremt over holdningen journalister har til digitalt kildevern og sier følgende: "Jeg tror ingen journalister sier at de sikrer seg godt nok. Kjetil Stormark er den eneste journalisten jeg vet om som kanskje er på et nivå som sikrer seg godt nok. Jeg gjør det definitivt ikke selv" (Brenna). Han mener det viktigste er at man vet at det kan spores. Man kan aldri være 100% sikker, men man kan gjøre det vanskeligere for kildejegerne.

Da Rønneberg bodde i Kina tok han flere forholdsregler under kontakten med kildene sine. Han var blant annet med på anskaffelsen av en kryptert varslingstjeneste til Aftenposten. På nettsiden www.varsle.aftenposten.no kan man sende kryptert informasjon til avisen slik at man kan avdekke lovbrudd og kritikkverdige forhold på en sikker måte. De anbefaler at man gjør dette fra en offentlig datamaskin som for eksempel fra en nettkafe. Her sier Aftenposten at de alltid verner om sine kilder og at man kan kontakte dem anonymt. Rønneberg gjorde blant annet følgende for å verne om sine kilder:

> Jeg sørger i hvert fall for å ikke bruke datamaskinen uten VPN når jeg besøkte Internettkafeer. Jeg var ikke like forsiktig hjemme, og det burde jeg kanskje ha vært. Dette var før nettskyer ble stort så jeg hadde ikke noe lagret her bortsett fra Gmail. Jeg brukte denne som primær e-mail. Jeg hadde det meste av filene mine lagret på fysiske disker (Rønneberg).

At Rønneberg hadde Gmail som primær e-post kan selvsagt ha ført til at han ble overvåket ettersom han var på listen over journalister som fikk e-postene sine sendt

videre til en ukjent avsender. Han sier også at han ikke sikret seg like godt hjemme som ellers, noe som er uforståelig. Sjansen for at man blir utsatt for dataangrep burde ikke være mindre hjemme enn offentlig, men heller tvert imot. Men det er tydelig at han stort sett tar sikkerhetshensyn og kommuniserer på måter som gjør det langt vanskeligere å kunne avsløre kilden.

> Jeg som mange andre journalister sørget for at hvis vi skulle ha sensitive samtaler gjorde vi det ikke på e-post eller gjennom direkte telefonkontakt. Vi koblet oss opp gjennom VPN linjer eller proxy-servere. "Hide my ass" eksisterte da også, og Skype ble også mye brukt for kommunikasjon. Vi trudde da at Skype ikke var mulig å overvåke for et annet lands myndigheter. (…) Man må sørge for at man kommuniserer på sikre linjer og at man utleverer dokumenter på en sikker måte ved å bruke TOR og den krypterte varslingstjenesten vår (Rønneberg).

Det har senere dukket opp sikkerhetshull i programvare til Skype. Russiske hackere fant et sikkerhetshull som gjorde at uvedkommende kunne få tilgang til kontoen din kun ved hjelp av e-postadressen din. Prosedyren som ble brukt tok bare noen få minutter og hackerne fikk da kontroll over din Skype-konto (NRK, 14.11.2012). Dette gjorde at Skype, som tidligere ble regnet som et svært sikkert kommunikasjonsprogram, fikk en strek i regningen og mange av deres brukere fikk hacket sine kontoer på en svært enkel måte. Det regnes fortsatt for å våre en trygg måte å kommunisere på, men ingenting er 100% trygt.

Det er selvsagt mulig å lagre informasjon sikkert på en datamaskin. Det tryggeste er å bruke den uten at den er tilknyttet Internett, samtidig som at man sikrer den godt. Dette vil minske sjansen for at dataene kommer på avveie betraktelig. Man må da enten bli utsatt for tyveri eller fysiske innbrudd dersom informasjonen skal havne i feil hender. Stormark er selv klar over at dette er den tryggeste måten å lagre informasjonen sin på. "Dersom jeg ikke er tilstede, er maskinene også offline. Jeg har en del enkle, men ganske greie huskeregler. Dersom informasjon ikke er online, kan den heller ikke hentes ut". Det skal ikke mer til for å gjøre informasjonen tryggere slik at man kan verne om kildene sine. Det vil være vanskelig å ha kontakt med kildene sine på en datamaskin uten Internett, men man kan jo lagre alt av sensitiv informasjon man har tilgang til på datamaskinen som er offline. Han bruker i tillegg kryptert harddisk slik at dataene blir vesentlig vanskeligere å gjøre forståelig selv for avanserte hackere.

> Da jeg begynte å arbeide opp mot hacker miljøet hadde jeg allerede kryptert harddisk og begynte å bruke VPN-forbindelse samtidig som jeg tok i bruk anonymiseringstjenesten TOR. Jeg brukte også noen av hackerne som rådgivere for hvordan jeg best kunne beskytte meg selv (Stormark).

Han brukte altså kunnskapen til noen av hackere til selv å sikre seg enda bedre. Dette er jo en kompetanse han kan ta med seg videre når han skal jobbe med journalistiske saker av stor offentlig interesse.

Som Almlid sa, oppgraderte Aftenposten datasikkerheten når de forstod at det fantes interesser som ønsker tilgang på Wikileaks dokumentene.

> Wikileaks-dokumentene lå på en lukket server som du bare kunne jobbe med via maskiner som ikke var på nettverket. Du måtte logge deg inn og dette ble loggført slik at vi hadde kontroll på hvem som hadde vært inne på systemet. Det var ikke mulig for noen å få tak i dokumentene, og dermed gjøre dem tilgjengelig for Internett. Det var helt umulig" (Almlid).

Det er aldri umulig å få tak i dataene, men de er mindre tilgjengelig når de er på en server som ikke er tilknyttet Internett. For en dreven sosial hacker ville dette vært en mulig oppgave dersom han fikk tilgang til å koble seg på det kablede nettverket. Det kunne også vært en utro ansatt som tok seg friheten med å spre denne informasjonen videre slik som Edward Snowden gjorde. Som Christian Probst sier er det eneste en hacker trenger for å komme seg inn på datasystemene, en ansatt som ikke kjenner bedriftens sikkerhetspolitikk til punkt og prikke.

Espen Andersen i NRK er tydelig på hva han mener er det viktigste journalister kan gjøre for å sikre sine data:

> Det er selvfølgelig viktig at du til enhver tid ikke bærer med deg mer data enn det du trenger. Altså la oss si at man må ta bort informasjonen som er sensitiv, og lagre det på et sikkert sted og ikke ha det med seg hvor enn man går (Andersen).

Dette er ganske enkle retningslinjer, men mange har i dag alle data tilgjengelige på ulike medium for å gjøre dataene mer oversiktlige og tilgjengelig. Ved å redusere informasjonen man bærer med seg er det også opplagt at tapet vil bli mindre dersom uhellet først er ute. Når det gjelder tekniske hensyn sier Andersen:

> Det ene er at jeg fulldiskkrypterer; dette er kanskje den viktigste tingen man kan gjøre. Bortsett fra å bruke tredjepartsprogramvare for å fulldiskkryptere hele pc-en. Ved å gjøre dette så er det i praksis umulig å få tilgang til dataene på disken (Andersen).

Når jeg spør om det er fokus på datasikkerhet i NRK sier Andersen at det er varierende IT-ferdigheter i de forskjellige redaksjonene. ”Ja både og, det varierer fra redaksjon til redaksjon. Der hvor jeg jobber er det definitivt det. Dette handler litt om kunnskapen, de ansatte må forstå at de ikke kan laste ned programvare de ikke kan stole på”. Ovenfra og ned i NRK er det mye fokus på datasikkerhet, men om disse instruksene blir fulgt er han ikke like sikker på. ”Man må lære seg at man ikke kan stole på e-poster og heller ikke klikke på linker man ikke vet hva inneholder. Dette handler mye om helt grunnleggende IT-ferdigheter”. At ansatte har ulike ferdigheter er jo ikke uvanlig, men datasikkerhet handler mye om sunn fornuft, og at man tar trusselen på alvor. Som Probst sier er det nok å ”lure” en ansatt. Dersom hackerne kommer seg inn på vedkommende sin datamaskin, har de som regel lett adgang til å rote rundt i deler av bedriftens data.

Rønneberg mener at datasikkerheten har blitt bedre de siste årene, og at varslingstjenesten som Aftenposten opprettet, har hjulpet veldig på. Den ble opprettet i samme periode som diskusjonen rundt DLD pågikk, og Aftenposten gikk på den måten ut og viste at de tar personsikkerheten på alvor. Datasikkerhet har også vært tema på SKUP-konferansen en rekke ganger de siste årene, og om dette sier Rønneberg: ”Jeg tror mange journalister er mer oppmerksomme på det nå enn før. Det har også vært et tema på SKUP i mange år nå, så jeg tror nok det har blitt bedre”. Den tidligere nyhetsredaktøren til Rønneberg i Aftenposten mener følgende om deres sikkerhet: ”Det var veldig stort fokus på det hele tiden. Det var spesielt stort fokus på det med Wikileaks-dokumentene, og det var sikkerhetsopplegg på høyt nivå hele veien” (Almlid). Det ville jo vært merkelig om en nyhetsredaktør skulle si noe annet, men det er flere av de intervjuede journalistene som har fremhevet måten Aftenposten sikret sine data på.

Det virker som Aftenposten sikret Wikileaks-dokumentene på en god måte ved å lagre dem på et lukket nettverk samtidig som de har en god varslingstjeneste som Rønneberg var med på å opprette. Rønneberg er usikker på hvor omfattende overvåkningen er og

sier at det aller meste av det han gjør som journalist kun vil gå ut over han selv, noe som har liten betydning mener han.

> Det hadde vært mye verre om en kilde hadde kommet i trøbbel på grunn av meg. (…) Det er jo ikke sikkert at kilden er klar over risikoen det innebærer å være en kilde eller en varsler, så det er jo viktig at man kommuniserer om det (Rønneberg).

Jeg skal nå gå litt nærmere inn på hva journalistene og IT-arbeiderne Anders Brenna og Espen Andersen mener om datasikkerheten blant journalistene i Norge. Kjetil Stormark, som også er svært opptatt av datasikkerhet, forteller og hva han mener er status blant dagens norske journalister.

Datasikkerhet blant journalister, en bløff eller prioritet?

Brenna mener datasikkerhet har vært et tema som har fått svært lite oppmerksomhet blant journalister og redaksjoner. Han sier følgende om fokuset på datasikkerhet: ”Det har aldri vært fokus på datasikkerhet. Det har vært veldig, veldig fraværende”. For å prøve å få journalister til å forstå hvorfor det er viktig å sikre seg på best mulig måte skrev han boken *Digitalt kildevern*. Boken skal gi kunnskap om hvordan journalister bør forholde seg i sin kommunikasjon med kildene. Det har vært laber interesse for boken, noe som sjokkerer Brenna selv. Han sier at journalistene må våkne og forstå hvordan de kan sikre kildene sine i et samfunn hvor informasjon lagres digitalt, og der kommunikasjon kan spores på måter som tidligere ikke var mulig. Det var da Aftenposten mottok Wikileaks-dokumentene datasikkerhet ble synliggjort mener han.

> Aftenposten hadde stort fokus på datasikkerhet da de hadde Wikileaks dokumentene, men det var første gangen jeg fikk høre om noen som tok det seriøst. De skjønte selv hva de satt på av informasjon og at den var ettertraktet, og det fikk de jo merke selv. Før dette har jeg knapt nok hørt om det (Brenna).

Espen Andersen som selv er svært opptatt av datasikkerhet og kildevern, sier følgende om hva som er fokusområdet når det gjelder datasikkerhet i NRK.

> Vi har en IT-instruks, men den går mer på nettverk, og på hva man installerer og bruker pc-en til. Den er ikke like opptatt av hvordan man tar vare på

> informasjonen på harddisken. Den har fokus på driftsmiljøet i NRK for å verne infrastrukturen, og ikke så stort fokus på kildevernet (Andersen).

At kildevernet ikke får stort fokus er jo ganske merkelig når man hører om hvor enkelt det er å komme seg inn på dagens medium som er dårlig sikret. Når man i tillegg har statistikker fra mørketalls-undersøkelsene om datasikkerhet, bør det kanskje ringe en bjelle om at det finnes utenforstående som kan følge deg uten at du selv merker det.

Stormark, som jobber med et nettverk bestående av journalister som driver journalistikk opp mot ekstreme grupperinger som begår alt fra terrorhandlinger og nedover, sier:

> Vi har egne folk både i Syria, Jemen og Egypt. Jeg har derfor forklart til de vi har kontakt med at de ikke kan jobbe med oss uten å bruke krypteringer som standard på e-post. Vi har derfor innført kryptering som standard, og forbud mot å bruke amerikanske systemer eller nettverk som enten er hostet eller rutet via USA (Stormark).

Han mener at gjennom dette prosjektet så har han muligens tredoblet antall journalister i Norge som bruker kryptering som standard. Da han jobbet for VG på slutten av 90-tallet prøvde han å innføre kryptering som standard, men dette var ikke mulig på grunn av dataplattformen VG brukte på den tiden. Han sier videre:

> Jeg tror ikke det er noen norske medieorganisasjoner som har noe forhold til kryptering i det hele tatt. Dersom de har det så er det noe de har begynt med nå i det siste. Jeg har tatt til ordet for at kryptering blir standard i norske redaksjoner (Stormark).

Han tar dermed svært viktige forholdsregler når han behandler sensitiv informasjon som kan ha stor interesse for kildejegerne. Det at han i tillegg mener å ha god innflytelse på andre norske journalister er jo også meget positivt. Han lever, i følge intervjuene jeg har gjort, opp til forventningene om å være en av journalistene som tar datasikkerhet svært alvorlig.

Med økte trusler utenfra og flere teknologiske enheter både privat og på jobb, må sikkerheten oppgraderes for å sikre kildene, og annet sensitivt materiale som journalistene har tilgang på. Jeg spurte derfor journalistene jeg har intervjuet om de

mener den digitale trusselen blir tatt på alvor. Med dette mener jeg at store mengder data lagres digitalt, og kommunikasjonen ofte blir lagret en eller annen plass slik at den kan spores. Enhver journalist vil være 100% bevisst på kildevernet og si at det er absolutt. De kommer aldri til å oppgi kilden de har lovet anonymitet, men er dette noe de klarer å overholde i dagens teknologisamfunn? Brenna mener at mye har blitt bedre etter Snowden-avsløringene.

> Men selv etter Snowden så står det veldig dårlig til med tanken om at det ikke holder å bare love noen anonymitet; du må også sikre kilden. Der stopper det opp for de aller, aller fleste fortsatt. Det er veldig lite bevissthet om at det er mulig å spore opp kilden (Brenna).

Aftenposten sikret Wikileaks-dataene på en lukket server, og daværende nyhetsredaktør Almlid mener det var de eldre journalistene som var de mest ivrige initiativtakerne til å sikre kildene best mulig. Dette er jo egentlig ganske merkelig når man tenker på at det er den yngre generasjonen som er født inn i den digitale tidsalderen. Har datasikkerhet blitt et glemt tema i utviklingen av stadig nye og mer avanserte teknologiske nyvinninger? Almlid sier følgende: ”Ja det gjorde de, spesielt de mest erfarne journalistene, det var dem som tok det mest på alvor. Og det var det noen av de yngre som også gjorde, men som kanskje måtte fortelles mer hvorfor vi gjorde det” (Almlid).

Andersen er i stor grad skeptisk til at man bærer med seg sensitive data til enhver tid, og ser spesielt faren dersom man skulle bli utsatt for tyveri, eller at man mister et medium med sensitive data. Han tror at flertallet av journalister ikke tar datasikkerhet på alvor, men tenker da ikke bare på at de kan bli utsatt for hackerangrep. ”Faren for at man mister pc-en er at digitale medier kommer på avveie. Da handler det om at man ikke kan gi garantier til sine kilder om at informasjonen ikke har lekket” (Andersen). Man må kunne forsikre kildene sine om at informasjonen som blir gitt blir mellom oss, og da mener Andersen at det er uforsvarlig å legge dataene på en åpen harddisk som er ukryptert. Han mener derfor at beskyttelsesnivået er fryktelig lavt. Brenna er inne på noe av det samme som Andersen sier om faren ved å få frastjålet eller miste et medium.

> Hvis en journalist får frastjålet mobilen så er det helt latterlig. Ved hjelp av disse IMEI-nummerene så er det helt håpløst for folk å bruke telefonen hvis den er

> stjålet. Hvis noen stjeler en journalist sin mobiltelefon så er det for å sjekke informasjonen og hvem du har ringt. Det er definitivt ikke for at telefonen er verdifull (Brenna).

Dette er jo selvsagt avhengig av hvilke hensikter mottakeren som får tilgang på telefonen har, og det er jo nødvendigvis ikke en person med vonde hensikter. Men som Brenna sier er nok verdien av informasjonen mye mer verdifull enn selve telefonen, dersom kildejegerne klarer å finne kilden som følge av at en journalist mister et medium. Rønneberg ønsker ikke å uttale seg om hvordan andre journalister tar hensyn til digitale trusler. Han sier også at det er lite av kommunikasjonen hans som er viktig, slik at han kan få trøbbel for det. Men dersom informasjonen er sensitiv så tar han selvsagt hensyn til kildevernet.

> Jeg kan ikke si så mye om hvordan andre journalister jobber eller hvilke hensyn de tar. Jeg er sikkert for naiv fortsatt, og jeg skulle tro det var en enkel sak for nesten hvem som helst enten privat eller offentlig å hacke seg inn på pc-en eller telefonen min for å se på hva jeg holder på med (Rønneberg).

Denne oppsummeringen tyder på at det enda er et stykke å gå før datasikkerheten blant journalistene er så god at kilden selv kan være trygg på at informasjonen ikke lekker. Verken måten journalistene sikrer sine data på eller måten den blir lagret på virker å være tilfredsstillende i dagens informasjonssamfunn. Det er bra at Snowden-avsløringene kanskje har åpnet øynene for mange journalister, men det handler om å gjøre de nødvendige tiltakene som fører til at befolkningen får nødvendig tillit til journalistene. Dersom tilliten er stor kan befolkningen fortsatt varsle om kritikkverdige forhold i samfunnet, for hva ville vel journalistikken vært uten tips fra publikum? Det gjenstår å se hva fremtiden bringer, men med nye dataangrep og skrekkhistorier i media så er det nok mange journalister som kommer til å forstå alvoret.

Datalagringsdirektivet

Kjetil Stormark bodde i New York under terrorangrepene 11. september og så på terrorhandlingen fra kontor-vinduet sitt. Etter den tid har vi opplevd 22. Juli, og begge deler er en påminnelse om at verden der ute ofte er et svært ubehagelig sted, sier han. Han mener derfor at vi må ha et system som kan være med på å beskytte landets innbyggere. Stormark har blandede følelser i forhold til innføringen av DLD og sier: ”Vi trenger et solid forsvar og en ordensmakt. Det er viktig at vi ikke er naive”. Han mener

det er naturlig å finne skjæringspunktet mellom det å forebygge terror og alvorlig kriminalitet, samtidig som at man ikke ender opp med å leve i et overvåkingssamfunn. Han holder for tiden på med å skrive en bok om beredskap, hvor han er inne på hvilken informasjon, metoder og registertilgang som er nødvendig og relevant for de som skal forebygge alvorlig kriminalitet og terror.

> Datalagringsdirektivet blir opplevd som viktig i eksempelvis PST. Spørsmålet er om vi har nok innsikt i forhold til hva slags data som er viktige for å kunne forebygge. Fra USA vet vi at dersom man gir NSA og andre anledning til selv å diktere hva de skal ha tilgang til av opplysninger, vil de jo ha alt. Det verken kan eller bør de få. Det vil støte viktige rettssikkerhetsverdier i et demokratisk samfunn (Stormark).

Han mener svaret kanskje er "ja", vi trenger et datalagringsdirektiv, men ikke for enhver pris. Han mener at det ikke er gjennomført en god nok kartlegging på om man faktisk trenger disse opplysningene man ønsker skal være tilgjengelig. PST kan helt sikkert ha nytte av DLD, men for personvernet og rettssikkerhetsmessige hensyn er direktivet problematisk. Han sympatiserer med den underliggende politiske analysen om at verden nå går i en antidemokratisk autoritær retning, og mener det var derfor han fikk tillit i hackermiljøene. Han mener DLD handler om hvilken verden vi ønsker å leve i, og at den uvitende allmennheten ikke har tatt inn over seg hva dette handler om.

> Wikileaks er jo et svar på dette. Jeg er ikke enig i at absolutt alle dokumenter nærmest usensurert skal legges ut på Internett, slik Wikileaks har gjort. Det er uansvarlig. Men jeg ser jo hva slags dynamikk som er i spill. Wikileaks er reaksjonen på en antidemokratisk utvikling internasjonalt. For hver bølge kommer det en motbølge (Stormark).

Rønneberg er også generelt skeptisk til alt som omhandler lagring av data.

> Det er fint at politiet skal forenkle jobben sin, og at det skal være mulig å fange forbrytere med digitale spor. Det er litt som NSA, man kaster et digert garn og satser på at noen er dumme nok til ikke å komme seg forbi det (Rønneberg).

Dette er samme problematikken som Espen Andersen tar opp når det gjelder hvordan Amerikanske myndigheter har brukt etterretningsinformasjonen. "Når du ser hvordan amerikanske myndigheter har brukt etterretningsinformasjon så er det helt opplagt at

den kan misbrukes" (Andersen). De skal jo ikke bruke denne typen informasjon før det er snakk om alvorlige ting, men det er ikke fokus på hva som brukes av overskuddsinformasjon som kommer frem etter slik overvåkning.

> Man ser hvordan politiet i dag bruker overvåkningsmetoder, som burde være forbeholdt veldig alvorlig kriminelle handlinger, til å oppklare hasjsaken til høyrepolitikeren Erik Skutle som var Erna Solberg sin vararepresentant. Dette skjedde jo nettopp på grunnlag av metadata/teledata (Andersen).

Han mener DLD er kjerneeksempelet på hvor naive politikerne kan være, og er selv personlig motstander av direktivet med tanke på problematikken rundt kildevernet. "Det er nettopp med tanke på kildevernet. Det har jo mye med personvernet å gjøre, men for meg og andre journalister vil det gi mindre kontroll over kildevernet". Andersen mener det er grunn for bekymring, og sier akkurat det samme som Rønneberg om å finne et påskudd til å fange en kriminell, "så kan man ta alle småfiskene rundt". Det er naivt å tro at denne type informasjon ikke vil bli misbrukt sier Andersen, noe NRK selv har fått oppleve.

> Vi har jo selv fått kjenne dette på kroppen i forhold til Klomsæt-saken hvor han ble beskyldt for å være kilde i forhold til lekkasje i Breivik-saken. Han ble avlyttet av politiet, og dette var ingen stor sak som endte opp med en bot på 20 000 kr til Klomsæt. Politiet benyttet seg allikevel av denne typen metoder. Så denne typen overvåkningsmetoder kommer til å bli misbrukt, og dataene kan bli brukt til andre ting enn hva de påstår i dag (Andersen).

Det var under 22. juli-rettsaken at Sigurd Klomsæt ble fratatt advokatbevillingen fordi han var anklaget for å ha lekket bilder av Anders Behring Breivik til pressen. Politiet hadde merket bildene med unike koder, og to av de lekkede bildene hadde Klomsæts kode på seg. Slik at de i denne saken fikk utlevert advokatens trafikkdata fra teleoperatøren. Politiet er etter loven avskåret fra å ransake slikt materiale når det kommer fra advokater og pressefolk. Klomsæt ble etter dette fratatt advokatbevillingen, men har hele tiden hevdet sin uskyld. Klomsæt selv mener det nå er opp til pressen og de seks redaktørene til mediene som publiserte bildene å se på hva dette betyr for kildevernet (Nettavisen, 12.02.2014).

> Det er åpenbart at pressen her har blitt lurt og latt seg misbruke. En verner nå en uredelig kilde, samtidig som en ser på at et justismord finner sted. Jeg vil innstendig oppfordre mediene til å gjøre en ny vurdering av hvilken informasjon de kan gi retten. De kan fortsatt avkrefte meg som mulig kilde, uten å peke på deres egentlige kilde, sier Sigurd Klomsæt (Ibid.).

Dette trenger ikke å være en lekkasje fra Klomsæts kontor, men kan også være en lekkasje fra politiet. Merkingen av bildene tok bare sikte på å avsløre eksterne lekkasjer, og ikke politiets egne. Steingrim Wolland som er tidligere juridisk rådgiver i Norsk redaktørforening mener her at "presseetikken *ikke* er til hinder for at den som måtte ha frifinnende opplysninger for Klomsæt, gir dette. Kildevernet er «absolutt» i relasjon til opplysninger som er gitt i fortrolighet, men det gjelder ikke for falske opplysninger gitt under misbruk av tillit" (Journalisten, 13.03.2014). Denne saken har skapt diskusjoner rundt kildevernet med tanke på opplysninger som ikke er gitt i fortrolighet, og som derfor ikke er underlagt kildevernet.

Anders Brenna mener at jo mer som lagres desto større er katastrofen dersom informasjonen kommer på avveie. Man kan aldri være 100% trygg og det gjør det farlig å kommunisere med digitale medium.

> Datalagringsdirektivet er en katastrofe for kildevernet. Informasjonen vil jo bli tilgjengeliggjort for enten PST eller andre myndigheter, så selv om teleselskapene er flinke til å holde på sitt, så tror jeg ikke det stopper amerikanske myndigheter i å få tak i informasjonen enten ved hjelp av loven eller ved hjelp av teknologi (Brenna).

Han mener man kan gjøre det vanskeligere å spore kilden ved å spre informasjonen ut over flere steder. Dette gjør det vanskeligere for eventuelle kildejegere å knytte sammen trådene sier han. "Dersom man legger alle eggene i en kurv som går via mobiltelefonen din er det enkelt å vite at hvis Anders Brenna er journalisten vi ønsker å fange opp, så er det bare å fange opp all kommunikasjon via mobiltelefonen" (Brenna). De som etterforsker journalisten sliter med samme dilemma som journalisten, dersom man har brukt mange kommunikasjonskanaler, og forskjellige medium. På samme måte er dette et dilemma for journalister som jobber med undersøkende journalistikk, når de skal knytte trådene sammen for å finne ut av krevende saker. Dermed kan journalister

beskytte seg med samme mekanisme for å trygge kildevernet. Så dersom DLD ser dagens lys, må journalister ta nye forholdsregler ettersom informasjonen som lagres der kan bli brukt mot dem på et eller annet tidspunkt.

Journalistrollen

Kildevernet i dagens teknologisamfunn

I Vær Varsom-plakaten er et av kravene å ikke oppgi kildens identitet når kilden selv har bedt om anonymitet. Dette er et av påbudene som journalistene må følge. Prinsippet er en meget sentral del av presseetikken, og man oppgir aldri kilden i disse sakene. I en del tilfeller er det ganske enkelt slik at det er nødvendig å holde kilden anonym for å kunne få frem viktig informasjon. Det hender at de som informerer pressen blir satt i en særdeles vanskelig situasjon dersom de deler informasjonen med allmennheten. Det er journalistens oppgave å videreformidle denne informasjonen i media, og for å oppfylle sin informasjonsoppgave må altså journalisten kunne love kilden anonymitet (Brurås, 2010, s.179). Det er helt klart at med flere medium tilgjengelig og med mye kommunikasjon på Internett blir kildevernet satt på nye prøver. Stormark sier følgende: "Problemet er at man har for dårlig teknisk innsikt til å kunne gjennomføre kildevernet i praksis. Det er jo det som på en måte er min bekymring". Med dette som utgangspunkt ønsker jeg å undersøke hva journalistene mener om status for kildevernet.

Rønneberg mener at det på samme måte som man går til legen eller psykologen og forteller om problemene man har, så har journalistene akkurat samme taushetsplikt i forhold til sine kilder slik at samtalen blir mellom dem. Han mener det er essensielt at denne tilliten eksisterer slik at kilden ikke blir avslørt og kan holde seg anonym når dette er nødvendig.

> Det er den hellige gral, altså man kødder ikke med kildevernet. Hvis man gjør det så har man jo null legitimitet. (…) Det skal være mulig å varsle for noen som vet om noe som ikke er riktig. Det kan for eksempel være et lovbrudd eller noe etisk uforsvarlig/problematisk som man ønsker å varsle om (Rønneberg).

Det er altså ingen tvil om at Rønneberg mener kildevernet er absolutt, og uten absolutt kildebeskyttelse vil jo kildene tørke ut. Dette har med tillitsforholdet mellom mediene og

deres kilder å gjøre. Almlid sier følgende: ”Det er 100%. Helt uten. Det er aldri et avvik i kildevern. Aldri”.

Det er altså ingen tvil om at kildevernet står ekstremt sterkt i journalistikken, lover man noe så holder man det, og noen ganger er det kanskje for absolutt? Spørsmålet er om det er så enkelt å love 100% anonymitet ved at kildene ikke løper noe risiko når de henvender seg til journalisten eller redaksjonen for å gi dem viktig informasjon. Stormark mener at kildevernet står like sterkt som tidligere, men utfordringene er absolutt tilstede. Han sier: ”Man har veldig dårlig næringsvett som journalist eller redaktør dersom du ikke har svært stor respekt for kildevernet, og det oppleves som et utenkelig regime” (Stormark). Han mener journalistene har spøkt vekk forsøkene på å ta forholdsregler, og undervurdert sikkerhetsbehovet for de tekniske løsningene. En av grunnene til dette mener han er fordi digitalt kildevern oppleves som overdreven forsiktighet som det ikke er grunnlag for. Brenna mener på sin side at pressen har sviktet kildevernet totalt, og at de ikke har stått oppreist og forsvart kildevernet.

> Man må huske på at flertallet av befolkningen var fra seg av begeistring av at politiet klarte å ta kilden til Breivikbildene. Flertallet er ikke på lag med journalistene i den saken. Journalistene har rett å slett sløst litt bort kildevernet og det er ikke populært nok (Brenna).

Han mener pressen har sviktet ved å være lavmælte i diskusjonen rundt DLD ettersom de ikke har skjønt konsekvensene av direktivet. Stormark har den samme oppfatningen, og har selv vært utsatt for heftig kildejakt en rekke ganger, samtidig som han har jobbet med etterretning i mange år. Han har også vært i kontakt med mange kilder som har stor egeninteresse av å gi veiledning i hvordan han kan beskytte seg selv og kilden. Når det gjelder status på kildevern til dagens journalister sier Stormark: ”Jeg vet hvor enkelt det kan være å krysspeile lekkasjer selv med tradisjonelle metoder. Det er nok litt for mye naivitet og kunnskapsløshet i redaksjonene knyttet til hvor lett det faktisk er å finne kildene som snakker med oss”. Dersom det ikke er mulig for en kilde å gi journalister opplysninger om kritikkverdige forhold så vil mediene slutte å motta sensitivt informasjon, legger han til. Dette er kanskje den viktigste faktoren for kildevernet, også ifølge Brenna.

> Pressen er totalt avhengig av å kunne få informasjon fra en totalt fremmed som de aldri har snakket med som tar kontakt nettopp fordi man er presset. Det er dette som gjør at man er uavhengig, man gjør en tillitsmannsjobb på vegne av samfunnet. Uten kildevernet er pressen redusert til å være en interesseorganisasjon som kunne skrevet sin egen blogg om hvorfor vi burde ha våre interesser (Brenna).

Det er ingen tvil om at tilliten mellom publikum og pressen er svært viktig for at varslerne skal henvende seg, og gi viktig informasjon til media. Stormark mener at det det er derfor varslingstjenester som Wikileaks har vokst frem. Nettopp fordi mediene ikke har klart å spille rollen sin slik de skal i demokratier.

> Mediene er helt avgjørende som et korrigerende element som avdekker maktmisbruk. Dersom denne korreksjonen ikke finner sted begynner demokratiene å utvikle seg i en nedadstigende spiral, og i en mer autoritær retning. Dersom maktapparatet i stadig større grad slipper unna med overtramp er det fristende å begå flere (Stormark).

Han mener at mediene i enkelte tilfeller bør sitte på avsløringene sine en stund før de blir publisert. Dersom man nylig har lagt igjen elektroniske spor er det for enkelt å legge sammen to og to for kildejegerne. Stormark mener at en av grunnene til at mediene har opplevd et frafall av kilder er noe som representerer et demokratisk kildeunderskudd. I teknologisamfunnet vi lever i har altså journalistene fått nye utfordringer å ta hensyn til for å bevare kildevernet, og tillitten til folket i demokratiet.

> Fremveksten av teknologisamfunnet gjør det så uendelig mye enklere å krysspeile elektroniske spor, hvor du har vært, hvem du har snakket med og dermed er det mye enklere enn før å rekonstruere hendelser. Selv hvis du er ganske avansert, er det ofte veldig krevende og nesten umulig å skjule sporene sine (Stormark).

Status om at kildevernet er ”absolutt” for en journalist er alle enige om, og som Andersen i NRK sier ”Man skal aldri bryte kildevernet, men dersom det står liv og helse på spill er det redaktøren sin jobb og vurdere hva som skal gjøres og ikke journalisten sitt ansvar”. Den journalisten som bryter med dette prinsippet vil ødelegge for tillitsforholdet både for seg selv og resten av pressen. Viktig samfunnsinformasjon vil dermed kunne holdes skjult for offentligheten, og som Rønneberg sier er dette journalistenes rolle. ”Det er å kaste lys på hva som skjer i samfunnet, altså fortelle hva som skjer”. Sakens kjerne er at alle i befolkningen skal kunne fremme synspunkter og

kritikk om nødvendig, under dekke av anonymitet (Brurås, 2010, s. 179). Det er kun fremtiden som kan vise hva det teknologiske samfunnet vil bety for kildevernet, men nye hensyn må tas og journalistene må være bevisste denne trusselen.

Fremtiden som journalist

At fremtiden blir enda mer digitalisert enn den er i dag, og at overvåkingssamfunnet blir mer fremtredende i et demokrati med ytringsfrihet kan man ikke se bort ifra. Internett er en gullgruve for mange av oss hvor man kan finne svar på det aller meste, men det har også sine ulemper. Finn Sjue sier følgende om informasjonskrigen på Internett:

> Den digitale teknologien er blitt høyhastighetsbanen for frakt av ufattelige mengder informasjon av alle slag. På mange måter så må nettet kalles menneskehetens store velsignelser i vår tid. Men som alt annet så har denne velsignelsen sin negasjon. Nettet kan også fungere som en forbannelse" (Sjue, 2011, s. 153).

Jeg har derfor spurt journalistene hva de tenker om fremtiden. Isolert sett så mener Brenna at journalistene har fått en bedre hverdag med Internett samtidig som det har blitt enklere å jobbe med gravejournalistikk. Han sier at kommentator i VG, Astrid Mæland, hadde et godt eksempel på hvordan Internett har forandret arbeidshverdagen til journalistene etter at hun hadde sett filmen om Watergate-skandalen. "Filmen kokes ned og alle sitter og blar i telefonkataloger for å finne telefonnumrene til folk, noe som da var gravejournalistikk. I dag så får man jo tak i dette uten problemer. Så mye har blitt enklere" (Brenna). Brenna mener at det har blitt ekstremt mye vanskeligere å beskytte seg selv og han tror ikke han hadde klart å beskytte "Deep Throat" kilden i Watergate dersom det hadde skjedd i dag.

> Til slutt måtte Deep Throat stå frem selv for at det skulle komme frem. Snowden hadde kommet til å blitt avslørt, og det var derfor han gikk ut og sa det. Han skjønte det ville komme frem at det var han, så den delen med gravejournalistikken er vanskeligere (Brenna).

Kjetil Stormark mener at det eneste innholdet som er sikkert er alt innhold som ikke er lagret digitalt, og som ikke er online.

> Når jeg skriver på sensitive manus så har jeg en egen datamaskin som aldri har vært online som jeg kjøpte på en sånn måte at den ikke kan ha blitt infisert av noe keystroke programvare eller noe som helst annet bug. Jeg lagrer ganske mye sensitive data på eksterne harddisker som igjen ligger i en safe, og som igjen er kameraovervåket med alarm (Stormark).

Etter å ha uttalt seg om dette til andre journalister har Stormark opplevd å bli latterliggjort i det journalistiske miljøet. Det viktigste er at han kan være 100% lojal mot kildene sine. Han vier derfor lite oppmerksomhet til hvordan sikkerhetsrutinene hans blir latterliggjort blant andre journalister. Han mener derimot at ting har blitt bedre etter avsløringene til Snowden, og at journalistene nå tar sikkerheten litt mer på alvor.

> Det har og å gjøre med den tekniske innsikten de forskjellige har, sånn at for meg så har det vært en lettelse at dette har blitt litt mer allmennkunnskap og blitt lettere å ta til orde for den varsomheten som faktisk er nødvendig (Stormark).

Vi er mye mer eksponerte enn før, sier Kristoffer Rønneberg. Det å kunne ha en privat samtale er mye vanskeligere enn tidligere. ”Nå må man nesten ta det for gitt at det man sier på telefonen vil/kan bli overvåket. (…) Det er mitt utgangspunkt at jeg ikke kan ha en privat samtale på telefonen” (Rønneberg). Han mener at man må ta det for gitt at det man sier på telefonen er offentlig tilgjengelig. Dette er sterke påstander, og det har ikke vært mange eksempler på at teledata har blitt brukt mot journalister her i Norge. At det kan bli brukt mot journalister og resten av befolkningen, er det derimot liten tvil om.

Journalistene vil ta større hensyn i fremtiden mener Almlid. Han mener det ikke bare handler om å oppgi kilden, men også hvordan man unngår å legge fra seg elektroniske spor slik at kilden ikke blåses gjennom uvettig bruk av digitale medier. Det er svært få journalister som er klar over hvor mye elektroniske spor som lagres, noe Almlid mener alle må bli mer bevisst på. Han tror også at det er mange journalister som ikke er klar over hvilken fare dette er for dokumentasjonen de sitter på. Dette er noe som også Andersen sier:

> Jeg tror at journalistene har en mer bevisst holdning i forhold til kildevernet, og det er nettopp fordi at de har fått en digital hverdagen. På den ene siden har vi fått journalister som er mer bevisst på farene samtidig som det har blitt vanskeligere å verne kildene (Andersen).

Han mener videre at det handler om hva slags informasjon som lagres om mennesker hos myndighetene og til andre aktører. Når kilden tar kontakt vil man automatisk kompromittere seg selv ettersom IP-adressen ligger lagret i loggen til telefonselskapet. Han tror problemet ligger like mye hos kildene som hos journalistene selv. Så bare fremtiden vil vise hvilke utfordringer journalistene står ovenfor, men med varsomhet og bevissthet av hvordan man kan spores, minsker man uansett sjansene for at kilden ikke kan holdes anonym.

Den journalistiske arbeidsmåten og praksisen

Med ny teknologi og digitalt lagret informasjon har journalistikken endret seg radikalt de siste tjue årene. Helt fra de første nettavisene ble publisert på midten av 90-tallet, har papirutgavene rast i opplag her i Norge. Avisene må tenke nytt om hvordan de skal tjene penger når reklameinntektene svikter, og med tradisjon med at nettutgavene har vært gratis har det blitt store kutt i mange mediehus. På samme måte har også måten journalistene jobbet på endret seg ettersom presset til å få publisert materialet så raskt som mulig er stort. Teknologien har endret landskapet journalistene jobber i, og mange snakker om at papiravisene vil forsvinne som en følge av digitaliseringen. Har teknologien endret journalistikken og måten man jobber på med tanke på kildevernet? Dette spurte jeg journalistene om.

Rønneberg som selv har opplevd overvåkning på flere måter sier at journalistene er mye mer eksponerte enn de var før, og at det å føre en privat samtale har blitt mye vanskeligere. Med alle avlytning-skandalene som har vært de siste årene friskt i minne, virker det som Rønneberg er meget klar over at det som sies på telefonen kan bli brukt mot han, og tar derfor hensyn til dette. ”Det er jo ikke verre enn at dersom jeg skal ha en privat samtale så går jeg bak en brannmur eller Skype. Uten at det er garantert at dette er sikrere så tenker jeg at det er et bedre alternativ” (Rønneberg). Dersom dette er utgangspunktet er det jo ganske opplagt at han er innforstått med problematikken dersom man jobber med noe sensitivt. At man da endrer måten kommunikasjonen foregår på og automatisk tar nye og andre hensyn, samt at man bruker andre kommunikasjonsmåter for å beskytte kildene sine.

Han er usikker på om den digitale verden vi lever i har endret journalistikken, men den har endret landskapet rundt oss. Rønneberg sier at folk ble avlyttet med analoge telefoner langt tilbake i tid også, slik at det på mange måter er de samme metodene som brukes i dag.

> Det har alltid vært sånn, telefonlinjer ble jo avlyttet for 50 år siden også. De prøvde også å unngå å bruke analoge telefonlinjer den gang slik at det er jo det samme prinsippet som vi opplever nå. Hvis man tenker på Watergate-saken så ville jo ikke Woodward eller Bernstein ringt rundt til kildene de jaktet på med vanlige analoge telefoner. Det er jo det samme prinsippet i dag (Rønneberg).

At man også tidligere måtte verne om sine kilder sår det liten tvil om, men med nye metoder og flere medium som har vokst frem de siste ti årene dukker det også opp nye utfordringer. Ole Erik Almlid er personlig tilhenger av digitale medier, og mener at det først og fremst er positivt for journalistikken. Med lettere tilgang til kildene og dokumentasjon som bare er noen tastetrykk unna, har det gitt journalistikken nye muligheter. Han mener også at det har dukket opp noen nye utfordringer for journalistene. "Det negative er at du kanskje blir litt naiv, og dermed får et behov for å endre journalistikkens utførelse. Da blir det viktig å tenke over hvordan man lagrer informasjonen fra kildene" (Almlid). Almlid mener at dette har vært med på å endre måten journalistene jobber på, men Kjetil Stormark er på sin side usikker på om journalistikken i det hele tatt har endret seg. "Han mener journalistene har vært naive og ikke forstått alvoret med digitalt kildevern.

> De fleste journalister har vært lykkelig uvitende om trusselen de har stått ovenfor, og har da ikke tatt de nødvendige forholdsreglene. Konsekvensene har vært at kildene er tause utenat journalistene har forstått hva som er grunnen til dette. Fordi at det er noen som går bakom journalisten og tetter igjen lekkasjene (Stormark).

Ifølge Stormark mister mediene mye av den korrigerende informasjonen, den som kommer inn andre veier enn maktapparatets offisielle håndtering av mediene dersom kildevernet ikke er godt nok. Kildene må kunne stole på journalistene og ta kontakt uten å være redde for at beskyttelsen som journalisten gir ikke er til å stole på.

> Når stadig mer av denne informasjonen blir borte, hvor folk er helt ærlige, da blir jo mediene i større grad manipulert og vi får servert redigert innhold på den

> måten som makta sjøl ønsker skal være det bildet som kommer ut. Man mister derfor styringen med informasjonsformidlingen og det er dypt problematisk når det stadig tas sånne små skritt. Dette er det store bildet som har med informasjonssikkerhet å gjøre (Stormark).

Brenna mener at journalistikken ikke har endret seg ettersom bevisstheten rundt kildevernet er fraværende. Har tror derimot at kildenes holdninger har endret seg for de som tidligere ville tipset journalistene. En annen konsekvens, som Brenna viser til, er at stadig flere kilder som henvender seg til pressen vil gjøre det med anonymiserte pakker som ikke journalisten får verifisert, noe som er et kjempestort problem i forhold til kildekritikken.

> Man kan ikke spore hvem vedkommende er fordi de ikke ønsker å være i kontakt med pressen. Det er nok av paranoide mennesker som har tippet over og som tror på det ene og det andre. Da er det vanskelig å skille ut om materialet er sant (Brenna).

Dette er en måte kildene kan slippe å stå til ansvar for sine påstander, og informasjon som ikke trenger å være tatt fra virkeligheten. Som Finn Sjue sier: ”Mange pressefolk har erfart hvordan anonyme kilder ønsker å bruke journalisten i en eller annen maktkamp eller intrige, der det er komfortabelt for kilden å opptre skjult. (Sjue, 2011, s. 153).

Det at man er i kontakt med kildene og samtidig får vurdert dem, er essensielt for journalisten. På denne måten kan man undersøke om kilden er til å stole på eller ikke. Man kan kommunisere og derfor ta et standpunkt til det kilden sier. Brenna mener at fremtidas gravejournalistikk blir å finne på Wikileaks dersom kildene ikke kan stole på media. Dette er nettsteder hvor det aldri kommer frem hvem som har kommet med informasjonen, og Brenna hevder denne kontakten er livsnerven til journalisten.

> Det er derfor vi har kildevern. Journalisten skal på vegne av samfunnet også kunne ha kontakt med kriminelle, for å kunne avdekke ting som ingen tør å stå frem med. Pressen kan ta grep ved å verifisere, men uten verifiseringsmuligheten ser det ikke bra ut (Brenna).

Andersen fra NRK sier at tidligere hadde journalistene med seg notatblokker som de låste inne. På den måten endres måten journalisten må sikre sine notater på. Han poengterer viktigheten med å sikre sine data når man har lovet kilden anonymitet. ”Jeg

tror ikke jeg ville ha lagret informasjonen på nettverket i det hele tatt bortsett fra i kryptert form. (…) Jeg har jo kollegaer som foretrekker penn og papir når de jobber med sensitive saker" (Andersen).

Kapitel 7 - Drøfting og konklusjon

I innledningen på denne masteroppgaven formulerte jeg følgende problemstilling: *Hvordan ivaretar journalister kildevernet i dagens digitale samfunn, og tar de tilstrekkelig hensyn til informasjonssikkerhet?* Ved å intervjue fem journalister om de samme temaene vil jeg i denne delen forsøke å oppsummere mine forskningsspørsmål ved å drøfte og gi en konklusjon på problemstillingen. Jeg stilte følgende tre forskningsspørsmål i innledningen av oppgaven.

- *Setter moderne kommunikasjonsløsninger kildevernet på prøve?*
- *Hvordan ivaretar journalister datasikkerheten når de frykter at de blir overvåket?*
- *Er kildevernet truet i dagens digitale samfunn?*

Setter moderne kommunikasjonsløsninger kildevernet på prøve?

I innledningskapittelet redegjør jeg for hvordan journalistene mener de ble utsatt for dataangrepet. De har alle forskjellige historier og opplevelser av dataangrepene de mener de kan ha blitt utsatt for. Det er svært vanskelig å sammenligne de ulike hendelsene ettersom de er ganske ulike. Jeg mener at svaret på spørsmålet om de har blitt angrepet eller ikke må ses i sammenheng med deres IT-kunnskaper. Slik jeg skrev i kapittelet om dataangrep kan verken jeg eller journalistene dokumentere at dataangrepene har funnet sted. Det betyr derimot ikke at ingen er ute etter å hacke en journalist eller at de er mindre utsatt enn andre samfunnsborgere.

Inntrykket jeg sitter igjen med etter å ha hørt historiene om hvordan informantene opplevde at dataangrepene fant sted, er at de er bevisste på hva som skjedde. Med gode IT-ferdigheter og stor bevissthet rundt hvordan teknologien kan brukes til kriminelle handlinger, er sjansen for at de har blitt utsatt for datakriminalitet tilstede. Datakriminalitet har blitt et verdensomspennende problem og sikkerhetstiltakene har ikke holdt følge med teknologiutviklingen. Som Bye & Sjue sier er de elektroniske og

automatiserte formene for overvåkning i ferd med å skyte kraftig fart. Datakriminaliteten skjer på enkle nivåer og styrken varierer avhengig av hva som er hensikten med overvåkningen.

Ny teknologi tas i bruk og med tydelige vinningsmotiv har datakriminaliteten blitt mer organisert enn tidligere. Jeg mener i likhet med Bye og Sjue at overvåkningen har blitt mer avansert, og at de teknologiske mulighetene er langt større en tidligere. At man også kan kjøpe slike tjenester fra organiserte kriminelle er skremmende. Med dette mener jeg at vi lever i en verden hvor det meste av moderne teknologi er tilknyttet Internett og mulig å nå for kriminelle. Utrolig mange enheter er tilknyttet det verdensomspennende nettverket, slik at store mengder informasjon er innenfor rekkevidde. Journalister som jobber med sensitiv informasjon som noen er på jakt etter, er nok ikke mindre utsatt enn andre samfunnsborgere. Med uante teknologimuligheter i dagens samfunn og data tilgjengelig på tvers av medium, er vi ekstra sårbare dersom uhellet først inntreffer.

Journalistene jeg har snakket med har alle opplevd forskjellige dataangrep som tyder på at de kan ha blitt utsatt for overvåking. Alle journalistene har lang erfaring, og viser stor interesse for datasikkerhet. Det er tydelig at datasikkerhet er noe de tar på alvor selv. De har opplevd ulike episoder hvor de har merket problemer med IT-utstyr, fått merkelige e-poster, eller blitt jaktet på av hackere. Almlid fikk etterforsket dataangrepet, og det ble senere sporet til Singapore mens Stormark fikk store driftsproblemer med sin datamaskinen under kontakten med LulzSec. Dette er kanskje de dataangrepene som tydeligst har funnet sted. Når det gjelder Rønneberg så har han vært på en liste på Gmailen som har blitt videresendt til en ukjent mottaker. Gmail ble i denne perioden hacket og mange fikk stjålet sine passord og tappet sine e-post kontoer. At Brenna har blitt hacket blir mest bare antagelser, men han har gode argumenter for hvorfor han mener han kan ha blitt utsatt for hacking, så man kan ikke utelukke noe som helst. Uten IT-kunnskapene til disse journalistene ville ikke noen av dataangrepene blitt observert. Hackerne er svært dyktige og jobber i skjul, slik at vedkommende som blir utsatt for dagangrepet aner fred og ingen fare.

Stormark som jobbet tett opp mot hackermiljøene har en erfaring som gjør han i stand til å forstå hva de er kapable til å utføre når det gjelder kriminelle handlinger på

Internett. Han mener at journalisters integritet ikke er sterkere enn at hackerne kan ha dem som mål i en kildejakt når man ser på hvilke andre dataangrep de har utført. Det er kildesensitivt materiale utenforstående kan ha interesse av å stjele dersom de skal hacke en journalist. Farene kan være mange, men mye av dette kan man unngå dersom man er klar over hva digitalt kildevern handler om. Som Brenna sier gjør man ingen tiltak dersom man ikke har oppdaget at noe dataangrep har inntruffet. Alle er enige om at moderne kommunikasjonsløsninger setter kildevernet på prøve. Jeg mener det samme som informantene når det gjelder at det digitale kildevernet ikke er godt nok selv om det har bedret seg etter avsløringene til Edward Snowden. Man skal ikke være paranoid i journalistrollen, men man må forstå at mulighetene er mange dersom noen ønsker å drive kildejakt. Hvis interessene er store nok kan kildejakten foregå på langt flere måter enn tidligere. Man må derfor ta nødvendige forholdsregler.

Hvordan ivaretar journalister kildevernet når de frykter de blir overvåket?

Det er tydelig at det er varierende hvor godt informantene mener at de beskytter seg selv mot dataangrep, og hvordan de ivaretar sikkerheten når de kommuniserer med kildene. Kildevernet er absolutt, noe som alle journalister står sammen om, men om det blir med praten eller om det tas nødvendige sikkerhetshensyn sår det tvil om. Som Brenna utalte er datasikkerhet innenfor journalistikken noe han knapt hadde hørt om før Aftenposten fikk tilgang til Wikileaks dokumentene i 2011. Dette er ikke mange år tilbake i tid, og teknologien med Internett som kommunikasjonsplattform har eksistert siden tidlig på 90-tallet. Alle informantene tar datasikkerhet på alvor, men derifra til hvilke tiltak de foretar seg varierer.

Brenna mener at Stormark er den eneste journalisten i Norge som sikrer seg godt nok med tanke på digitalt kildevern. Stormark gjør en rekke sikkerhetstiltak, men har selv opplevd å bli sett på som paranoid og blitt latterliggjort i det journalistiske miljøet når han forteller om sine metoder for å beskytte kildene. Han bruker kryptering som standard sammen med de andre journalistene jeg har intervjuet, og fremhever også at det enkle ofte er det beste ved at man kobler fra Internett-tilgangen. Dette var også prosedyren Aftenposten fulgte da de satt på Wikileaks-dokumentene, og da er det tilgangen de ansatte har til det lukkede nettverket som må begrenses i størst mulig grad

for å sikre dataene. Andersen mener det i stor grad handler om helt grunnleggende IT-ferdigheter som for eksempel å ikke trykke på linker i e-poster som man ikke har kjennskap til. Flere av journalistene jeg har snakket med har også vært pådrivere for å få andre journalister til å bruke kryptering, og sikker kommunikasjon mot ulike medier. Journalistene benytter seg også av VPN-linjer og proxy-servere for å kunne kommunisere på en trygg måte.

Gjennom SKUP-konferansen har datasikkerhet og undersøkende journalistikk på Internett vært et tema i mange år slik at tematikken etter hvert er velkjent for de fleste journalistene. Når man selv forstår hva som er mulig å få tak i av informasjon på Internett, og ser hvilket utrolig hjelpemiddel dette kan være, så bør man forstå at det også kan brukes med vonde hensikter. Tore Ordløkken (2010) ved Norsk senter for informasjonssikring sier at det er enkelt å tro at Journalister er mer opptatt av datasikkerhet enn andre, men dette er det vanskelig å finne gode holdepunkter for. Når det gjelder journalistene jeg har snakket med, mener jeg at de ivaretar datasikkerheten på en forsvarlig og god måte ved at de gjør en rekke sikkerhetstiltak.

Når det gjelder datasikkerheten blant journalistene ellers i Norge har informantene varierte meninger om den er god eller ikke. Det alle er enige om er at bevisstheten rundt digitalt kildevern, og måten man beskytter seg på kan bli mye bedre. Stormark mener at kryptering bør bli standard i alle norske medieorganisasjoner, noe jeg er enig med han i. Det kan virke som om datasikkerhet er noe som blir oversett av mange journalister og Brenna sier at datasikkerheten er fraværende og lite prioritert. Overvåkningen er overalt rundt oss, så da gjenstår det å se om Sjue (2011) får rett når han mener at naiviteten råder og at kunnskapene om de ulike formene for overvåkning er svake. Skal vi beholde journalistene som vaktbikkjer i et samfunn som trenger undersøkende journalistikk, trenger også media tilliten til befolkningen.

Er kildevernet truet i dagens digitale samfunn?

Det er fortsatt usikkert hva som skjer med DLD etter at EU-domstolen har konkludert med at direktivet er i strid med EUs charter om grunnleggende rettigheter. Direktivet er vedtatt i Stortinget får tiden vise om direktivet blir innført eller ikke. At et slikt direktiv

kan brukes til å finne eventuelle kilder, har vi sett et eksempel på i Klomsæt-saken. Her ble jo også teledata fra kommunikasjonen han hadde hatt med journalistene brukt for å finne ut hvem han hadde hatt kontakt med. Informantene er uenige om dette er et direktiv som er nødvendig eller ikke. De har alle forståelse av at alvorlig kriminalitet som terror må bekjempes, men er samtidig usikre på hvordan et slikt direktiv vil bli brukt, og hva som skjer med overskuddsinformasjonen? Vi fikk jo også et eksempel på det i hasj-saken med høyrepolitikeren Erik Skutle som ikke er en sikkerhetstrussel mot andre mennesker. All informasjon som lagres og samles kan bli brukt mot oss i fremtiden. Hvem som har tilgang og hvordan de benytter seg av informasjonen er uvisst, og derfor kan det være en stor trussel for kildevernet. Fremveksten av teknologisamfunnet gjør det uendelig mye enklere å kryssjekke spor sier flere av journalistene, noe jeg støtter dem i. Med enkle metoder kan man finne mange løse tråder som til slutt fører frem til målet som da kan være kilden.

Rønneberg bruker sterke ord når han sier at man nesten må ta for gitt at det man sier på telefonen kan/vil bli overvåket. Dersom man har dette som utgangspunkt må man ta nye hensyn og være klar over konsekvensene som kan oppstå for journalistene dersom kildevernet kompromitteres. Mørketallsundersøkelsene viser at sikkerheten er sviktende, og at det er få tegn til forbedring. Ser man dette i sammenheng med det som Tjaberg i NSM sier om at nye medier har gjort oss mer sårbare en noen gang, så er det ikke tvil om at kildevernet kan være truet. Andersen mener at journalistene er mer bevisste på farene, men at det har blitt vanskeligere å verne kildene. Det er derfor nødvendig å være varsom og fornuftig slik at man kan videreføre tilliten journalistene har til befolkningen.

Den journalistiske arbeidsmetoden og praksisen forandres på den måten at man må tenke mer over hvordan man kommuniserer med kildene sine, og samtidig sikrer sine data på en god måte. Dersom kildene ikke tør å kontakte pressen vil det oppstå flere varsler-nettsteder som Wikileaks, som mottar enorme pakker med anonymisert informasjon. Hva ville Wikileaks vært uten journalistene? Noen må behandle informasjonen, men samtidig må varslerne kunne holdes skjult. Hvem kan stole på journalistene dersom det kommer frem at datasikkerheten holder et svært lavt nivå, og hva vil dette bety for fremtidens gravejournalister? Kanskje får vi svar på dette i årene

som kommer. En ting jeg er sikker på er at det finnes interesser der ute som er ute etter informasjon og data som pressen har tilgang på. Hvilke metoder disse kildejegerne benytter seg av er uvisst, men at fremtidens overvåkningsmetoder blir mer avanserte og automatiserte, er det mange eksempler på. Journalistene skal selvfølgelig ikke slutte å kommunisere ved hjelp av teknologi eller være redde for å lagre dataene de jobber med. Det eneste som må gjøres er å øke bevisstheten rundt digitalt kildevern, samtidig som sikkerhetstiltakene blir iverksatt. Dette er med forbehold om at kildene fortsatt kan kontakte pressen med trygghet om at de er anonyme.

Litteratur

Aftenposten, 06.04.2011: *"9 av 10 solgte mobiler er en smarttelefon"*. URL: http://www.aftenposten.no/digital/nyheter/9-av-10-solgte-mobiler-er-en-smarttelefon-6279888.html [Lesedato: 04.03.2013]

Aftenposten, 12.10.2011: *"250.000 nye Wikileaks-dokumenter til Aftenposten"*. URL: http://www.aftenposten.no/nyheter/uriks/wikileaks/article3953048.ece [Lesedato: 01.03.2013]

Aftenposten, 16.11.2011: *"Offentlig datasikkerhet er en stor bløff"*. URL: http://www.aftenposten.no/nyheter/iriks/--Offentlig-datasikkerhet-er-en-stor-bloff-6699134.html [Lesedato: 06.03.2013]

Bodal-Johansen, Gunnar (1995). *Presseetikk fra a til å*: I kortversjon. Institutt for Jornalistikk

Brenna, Anders, 04.01.2011: *"Slik fikk Aftenposten WikiLeaks"*. URL: http://blogg.abrenna.com/slik-fikk-aftenposten-wikileaks/ [Lesedato: 12.03.2013]

Brenna, Anders (2012). *Digitalt kildevern*. Kristiansand: IJ-forlaget.

Brurås, Svein (2010). *Etikk for journalister.* (4. utg. ed.). Bergen: Fagbokforlaget.

Bye, Ronald & Sjue, Finn (2008). *Overvåket*. Oslo: Gyldendal akademisk.

Dagbladet, 19.01.2010. *"Google hacket sine egne"* URL: http://www.dagbladet.no/2010/01/19/nyheter/utenriks/google/google_china/9995111/ [Lesedato: 05.03.2014]

Dagbladet, 19.02.2013: *"I dette bygget ligger Kinas hackingsentral"*. URL: http://www.dagbladet.no/2013/02/19/nyheter/utenriks/kina/hacking/25833595/ [Lesedato: 07.03.2013]

Daler, Torgeir., Gulbrandsen, Roar., Høie, Tore Audun., & Sjølstad, Torbjørn (2010). *Håndbok i datasikkerhet*: informasjonsteknologi og risikostyring (3. utg. ed.). Trondheim: Tapir akademisk.

Datatilsynet, 27.11.2011: "*Datatilsynets oppgaver*". URL: https://www.datatilsynet.no/OmDatatilsynet/Oppgaver/ [Lesedato: 04.05.2014]

Datatilsynet, 18.12.2012: "*Nettskytjenester - Cloud Computing*". URL: https://www.datatilsynet.no/verktoyskjema/Publikasjoner/Veiledere/Nettskytjenester---Cloud-Computing/ [Lesedato: 04.03.2014]

Datatilsynet, 08.04.2014: "*Nå må den norske loven gjennomgås*". URL: https://www.datatilsynet.no/Nyheter/2014/-DLD-et-alvorlig-inngrep-i-privatlivet/ [Lesedato: 04.03.2014]

Digi, 07.03.2012: "*Lulzsec-sjef var FBI-informant*" URL: http://www.digi.no/891264/lulzsec-sjef-var-fbi-informant [Lesedato: 04.04.2014]

Forskning, 08.11.2012 - 09.03.2013: "*Du er det svakeste leddet i it-sikkerheten*". URL: http://www.forskning.no/artikler/2012/november/338483 [Lesedato: 09.03.2013]

Fossum, Egil & Meyer, Sidsel (2008). *Er det nå så sikkert?*: Journalistikk og kildekritikk. (3. utg. ed) Cappelen Fkademsik Forlag.

Gottschalk, Petter (2011). *Datakriminalitet i Norge*. Unipub

Harding, Luke (2014). *Snowden-Filene*: Historien om verdens mest ettersøkte mann. Forlaget PRESS

Hardware, 27.06.2004: "*GUIDE: IP-adressering*". URL: http://www.hardware.no/artikler/ip-adressering/1623 [Lesedato: 02.03.2013]

Hardware, 30.07.2009: "*Mac mer utsatt for innbrudd*". URL: http://www.hardware.no/artikler/mac_mer_utsatt_for_innbrudd/71072 [Lesedato: 04.03.2013]

Hardware, 30.12.2010: "*Datainteresserte ute etter lulz og en bedre verden*". URL: http://www.hardware.no/artikler/anonymous_under_lupen/80225 [Lesedato: 04.03.2014]

Hardware, 12.11.2012: "*Lur nettsperren med proxy og VPN*" URL: http://www.hardware.no/artikler/dette_trikset_hater_nettbransjen/93555 [Lesedato: 17.04.2014]

Hjeltnes, Guri & Warmedal, Morten Møller (2012). *Gravende journalistikk*: metode, prosess og etikk. Oslo: Gyldendal akademisk.

International Data Group, 16.09.2011: "*iPad det sikreste nettbrettet*". URL: http://www.idg.no/macworld/article220743.ece [Lesedato: 05.03.2013]

International Data Group, 23.01.2012: "*Trådløse nett like sikre som kablede*". URL: http://www.idg.no/computerworld/article236405.ece [Lesedato: 09.03.2013]

ITavisen, 31.01.2013. "*Stjal passordet til samtlige journalister*". URL: http://www.itavisen.no/910611/stjal-passordet-til-samtlige-journalister 07.03.2013%5D [Lesedato: 10.03.2013]

Johannessen, Asbjørn., Tufte, Per Arne & Kristoffersen, Line (2006). *Introduksjon til sammfunnsvitenskapelig metode.* Abstrakt forlag

Journalisten, 10.02.2010. "*Angrepet fra Tyrkia*". URL: http://www.journalisten.no/story/60479 [Lesedato: 07.03.2013]

Journalisten 13.03.2014 "*Klomsæt-saken og kildevernet*" URL: http://www.journalisten.no/node/41843 [Lesedato: 17.04.2014]

Krumsvik, Rune Johan (2013). *Innføring i forskningsdesign og kvalitativ metode*: Kompendium. Fagbokforlaget.

Lindahl, Ina (2009). *Massemedienes kildevern : en lærebok*. Bergen: Fagbokforlaget.

Lovdata. *Lov om styrking av menneskerettighetenes stilling i norsk rett*. URL: http://lovdata.no/dokument/NL/lov/1999-05-21-30[Lesedato: 08.05.2014]

Mandiat (2013). *Exposing One of China´s Cyber Espionage Units.* URL: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [Lesedato: 18.03.2013]

Miller, Charles & Dai Zovi, Dino A., (2009). *The Mac hacker's handbook*. Indianapolis, Ind.: Wiley Pub.

Nasjonal sikkerhetsmyndighet, 17.11.2011, 06.03.2012. "*NSMs sikkerhetskonferanse 2011 - Nasjonal sikkerhetsmyndighet*". URL: https://http://www.nsm.stat.no/Aktuelt/Nytt-fra-NSM/NSMs-sikkerhetskonferanse-2011/ [Lesedato: 06.03.2013]

Nettavisen, 12.02.2014. "*Klomsæt dømt for lekkasjer*" URL: http://www.nettavisen.no/nyheter/3754904.html [Lesedato: 05.04.2014]

Norsk senter for informasjonsikring, 09.09.2010, 18.03.2013. "*NorSIS - Fire av ti bryr seg ikke*" URL: http://www.norsis.no/nyheter/2010-09-09-Fire-av-ti-bryr-seg-ikke.html [Lesedato: 18.03.2013]

NRK, 14.11.2012. "*Skype-kontoer kan hackes ved hjelp av epost-adresse*" URL: http://www.nrk.no/viten/hacker-skype-med-epost-adresse-1.8396033 [Lesedato: 11.04.2014]

NRK, 26.10.2013. Spiegel: *"Merkel kan ha vært overvåket"* i 10 år. URL: http://www.nrk.no/verden/_-merkel-overvaket-i-ti-ar-1.11321280 [Lesedato: 09.05.2013]

NRK, 02.04.2014. "*Dømt for hackerangrep mot Ap*". URL: http://www.nrk.no/ostlandssendingen/domt-for-hackerangrep-mot-ap-1.11644911 [Lesedato: 05.04.2014]

Norsk Presseforbund. (2013). *"Vær Varsom-plakaten".* URL: http://presse.no/Etisk-regelverk/Vaer-Varsom-plakaten [Lesedato: 12.03.2013]

Ny Tid, 19.06.2004. "*Forsvaret fikk en ukritisk presse*". URL: http://no.wikipedia.org/wiki/Ikkevold-saken [Lesedato: 02.05.2014]

Næringslivets Sikkerhetsråd (2012). *Mørketallsundersøkelsen* - Informasjonssikkerhet og datakriminalitet. URL: http://www.nsrorg.no/getfile.php/Dokumenter/NSR%20publikasjoner/Mørketallsundersøkelsen/moerketall_2012.pdf [Lesedato: 07.03.2013]

Online, 01.06.2012. "*1 million nordmenn med nettbrett*". URL: https://www.online.no/teknologi/1_million_nordmenn_med_nettbrett.jsp [Lesedato: 14.03.2013]

Ottosen, Rune & Krumsvik Arne (2008). *Digitale medier og redaksjonell endring*. Journalistikk i en digital hverdag. Kristiansand: IJ-forlaget

Politiet, "*Datakriminalitet*". URL: https://www.politi.no/rad_fra_politiet/datakriminalitet/ [Lesedato: 05.05.2014]

Post og teletilsynet. (2012). *Tilsynsrapport - tilsyn med UNINETT Norid AS*. URL: http://www.npt.no/teknisk/internett/domene/norske-domenenavn-er-sikre-og-stabile [Lesedato: 05.04.2014]

Rosenbach, Marcel, Stark Holger & Guro Sandnes (2011). *Statsfiende WikiLeaks:* korleis ei gruppe nettaktivistar utfordrar ein av dei mektigaste nasjonane i verda. Oslo: Samlaget.

Sjue, Finn (2011). *Undersøkende journalistikk : en innføring*. Kristiansand: IJ-forlaget.

Store norske leksikon, "*Den kalde krigen*". URL: http://snl.no/Den_kalde_krigen [Lesedato: 03.05.2014]

Store norske leksikon, "*Informasjonssikkerhet*". URL: http://snl.no/informasjonssikkerhet [Lesedato: 05.05.2014]

Telenor, 01.06.2012. "*1 million nordmenn med nettbrett*". URL: http://www.online.no/teknologi/1_million_nordmenn_med_nettbrett.jsp [Lesedato: 04.03.2013]

Thagaard, Tove (2009). *Systematikk og innlevelse* : En innføring i kvalitativ metode. (3. Utg. ed.) Fagbokforlaget.

Tjora, Aksel (2012). *Kvalitative forskningsmetoder i praksis*. (2. Utg.ed) Gyldendal akademisk.

Trendmicro (2012). *Russian underground* 101. URL: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf [Lesedato: 12.03.2013]

TV 2, 21.01.2011. "*Kina skal ha partivennlig presse*". URL: http://www.tv2.no/nyheter/utenriks/-kina-skal-ha-partivennlig-presse-3393708.html [Lesedato: 05.05.2014]

TV 2, 06.11.2011. "*Aftenpostens nyhetsredaktør utsatt for hackerangrep*". URL: http://www.tv2.no/nyhetene/innenriks/aftenpostens-nyhetsredaktoer-utsatt-for-hackerangrep-3381765.html [Lesedato: 03.05.2014]

TV 2, 16.12.2011. "*Slik unngår du at mobilen din blir hacket*". URL: http://www.tv2.no/gmn/slik-unngaar-du-at-mobilen-din-blir-hacket-3537121.html [Lesedato: 02.03.2013]

TV 2, 14.02.2012. "*Nordmenn er de mest digitale i verden*". URL: http://www.tv2.no/nyheter/innenriks/nordmenn-er-de-mest-digitale-i-verden-3987156.html [Lesedato: 06.03.2013]

TV 2, 21.03.2013. "*Journalister ble ulovlig overvåket*". URL: http://www.tv2.no/a/4013659 [Lesedato: 03.04.2013]

VG, 24.01.2001. "*Rekordstreng straff til datasnoker*". URL: http://www.vg.no/teknologi/artikkel.php?artid=1089136 [Lesedato: 07.03.2013]

VG, 31.05.2005. *"- Ja, Felt var «Deep Throat»".* URL: http://www.vg.no/nyheter/utenriks/ja-felt-var-deep-throat/a/279313/ [Lesedato: 07.03.2014]

VG, 06.04.2011. "*Politikere hetses og trues etter datalagrings-ja*" URL: http://www.vg.no/nyheter/innenriks/arbeiderpartiet/politikere-hetses-og-trues-etter-datalagrings-ja/a/10091764/[Lesedato: 15.03.2014]

Østbye, Helge., Knapskog, Karl., Helland, Knut & Larsen L Leif Ove (2007). *Metodebok for mediefag*. (3. Utg. ed.) Fagbokforlaget.

Østlyngen, Trine & Øvrebø, Turid (2006) *Journalistikk*: Metode og fag. (2. Utg ed.) Oslo: Gyldendal akademsik

Muntlige kilder – forskningsintervjuene

Det er intervjuet fem journalister. De er valgt ut fra at de oppfyller kriteriene mine for casestudiet, eller at de representerer journalister med høy IT-kompetanse/utdanning slik at jeg kan belyse casene fra et annet perspektiv.

Intervjuobjekt	**Data**	**Rolle**
Kristoffer Rønneberg	11. mars 2014	Journalist og korrespondent for Aftenposten i New York, tidligere Beijing
Ole Erik Almlid	17. mars 2014	Tidligere nyhetsredaktør i Aftenposten
Espen Andersen	17. mars 2014	Journalist, forfatter og programmerer i NRK Brennpunkt
Anders Brenna	26. mars 2014	Frilansjournalist og forfatter med IT-utdanning
Kjetil Stormark	26. mars 2014	Frilansjournalist og forfatter

Vedlegg

Intervjuguide

1. **Hacking**

- Hvordan oppdaget du at du ble hacket?
- Hva tenkte du når du oppdaget det?
- Hvem trur du kan stå bak datainnbruddet?
- Har du noen tanker om hvorfor de hacket akkurat deg?
- Hvilken informasjon trur du at hackerne var ute etter?
- Hvilken skade gjorde de/dem?
- Har du opplevd noe lignende tidligere?

2. **Datasikkerhet**

- Hva gjør du for å sikre dataene dine?
- Tar du sikkerhetstrusselen på alvor?
- Er det fokus på datasikkerhet i din mediebedrift?
- Føler du at du er godt nok beskyttet?
- Tar dagens journalister den digitale trusselen på alvor?
- Hva lærer dere om datasikkerhet i din bedrift og har dere konkrete retningslinjer?
- Hva tenker du om innføringen av Datalagringsdirektivet?

3. Journalist yrket

- Hva er din viktigste rolle som journalist?
- Hvor sterkt er kildevernet?
- Hvorfor er kildevern viktig?
- Hvem kan være interesserte i å hacke en journalist?
- Hvilke konsekvenser kan det få for deg som journalist dersom noen får tilgang på alle dine data?
- Hvilke forhåndsregler tar du når du skal beskytte en kilde
- Hvordan trur du fremtiden blir når alle data er digitale?

4. Den journalistiske praksisen og arbeidsmåten

- Har det du har opplevd endret måten du jobber journalistisk på? Hvordan?
- Er det saker eller stoffområder du nå er mer skeptisk til å gå inn i fordi du er bekymret for overvåking og hacking og for både egen og kilders sikkerhet? Forsvarssaker? Etterretningssaker? Politikk? Krimsaker?
- Endrer trusselen om hacking og overvåking journalistikken på noen måte? Hvordan?
- Er dette først og fremst et problem for redaksjoner med små ressurser både materielt og menneskelig?