Internasjonal POLITIKK Årgang 72 | Nr. 2 | 2014 | 253–262 | ISSN 0020-577X

FOKUS: TEKNOLOGISERINGEN AV HUMANITÆRT ARBEID

«Do no harm»: Samtykke og personvern i krise?

CHRISTOPHER WILSON
M.A., Knowledge Lead, the engine room
wilson@theengineroom.org

Med utgangspunkt i det humanitære imperativet om at humanitær innsats ikke må gjøre skade eller utsette mottagerne for risiko, ser dette bidraget på en spesifikk side ved digitalt hjelpearbeid, nemlig hvordan vi skal forstå kravene til personvern og samtykke i krisesituasjoner.

Mobil- og nettbaserte informasjons- og kommunikasjonsteknologier har skapt nye muligheter for både innhenting og bruk av informasjon i humanitært arbeid. Mens nye verktøy skaper nye muligheter, skapes også nye utfordringer.

Mer og bedre informasjon kan brukes til forebyggende varsling, rapportering, logistikk og koordinering og til såkalt 'spillifisering'.[1] Tross stor teknologi-optimisme er det likevel usikkert hva som er informasjonsteknologiens mulige og faktiske bidrag i humanitære kriser. Samtidig er det en økende anerkjennelse av at sanntidsutveksling av informasjon, store mengder metadata («big data») og lav kapasitet til å analysere og prosessere informasjon skaper uventede risikoer og utfordringer når det gjelder personlig samtykke og personvern. Utfordringer knyttet til personvern, særlig samtykke og anonymisering, er velkjent fra tradisjonell humanitær bistand, og har lenge vært gjenstand for politisk debatt. Ny teknologi bringer likevel med seg nye problemstillinger: informasjon sprer seg raskt og ukontrollert, gjenbruk og modifisering kan fortsette i det uendelige, og det digitale skillet speiler også ofte partsforholdene i konflikter.

Implikasjonene av disse problemstillingene for personvern og samtykke har bare så vidt blitt tatt opp i den humanitære diskursen. Ett av de viktigste bidragene til den innflytelsesrike OCHA-rapporten *Humanitaria-*

1. «Gamification» er en prosess hvor spillteori og -metoder brukes til å løse problemer i andre sektorer (definisjon basert på The Gamification Summit 2012, sitert i Zeineddine 2012).

nism in the Network Age (2013) er at den henviser til viktige problemstillinger som oppstår rundt personvern, etikk og sikkerhet. Men rapporten går ikke så langt som til å knytte problemstillinger rundt bruk av digital informasjon til det tradisjonelle kravet hos humanitære aktører om at informasjon må brukes etisk og på en måte som ivaretar de humanitære aktørenes beskyttelsesansvar.

Denne lenken kan være krevende å knytte, ettersom fri flyt av digital informasjon på tvers av aktører og plattformer kompliserer spørsmål om eierskap, kontroll og ansvar. I humanitære kriser finnes det ikke alltid et direkte forhold mellom de som formidler og bruker informasjon og de som har gitt fra seg kunnskap, observasjoner eller data, eller som omtales i rapporter og meldinger. I forbindelse med humanitære kriser deles fotografiske fremstillinger av lidelse og desperate bønner om hjelp på sosiale medier. Åpning av biometrisk eller «big data» for koordinering kan støtte overvåking og eventuelle menneskerettighetsbrudd overfor tredjeparter. Spørsmål om ansvar og eierskap til denne type informasjon er spesielt krevende (se Iacucci 2013; Hosein & Nyst 2013).

I de fleste humanitære kriser kan det argumenteres med at det humanitære mandat allerede inneholder et direkte ansvar for å beskytte grupper og individer som gir fra seg informasjon eller er omtalt i denne. Dette ansvaret har fire beslektede delområder: 1) identitet og anonymitet;[2] 2) samtykke; 3) kontroll;[3] og 4) gjenbruk av data og informasjon.

For hvert av disse underområdene eksisterer det allerede humanitære retningslinjer. Av disse fire er det samtykke-kategorien som er mest utviklet som etisk begrep, samtidig som implikasjonene for humanitær praksis og ansvar i et digitalt informasjonslandskap er mest usikre. Denne artikkelen vil derfor se nærmere på dette begrepet og hvordan det operasjonaliseres i det digitaliserte humanitære arbeidet. I det følgende diskuteres først, med utgangspunkt i helseforskning, hvordan standarder for samtykke har utviklet seg. Deretter ser jeg nærmere på dagens informasjonsøkologi i humanitær praksis og potensielle farer ved å samle og bruke informasjonen veid opp mot muligheten for mer effektiv og målrettet nødhjelp. Bidraget konkluderer med at behovet for retningslinjer og kjøreregler for bruk av informasjon i kriser er sårt tiltrengt, og gir noen konkrete steg videre i denne prosessen.

2. Almon & Farkas (2013) presenterer en oversikt på risikoer knyttet til identitet og fortrolig informasjon i humanitære tiltak samt noe mulig respons for humanitær aktører.

3. Individers kontroll over når og hvordan data om dem blir bruk, eller *informational self-determination*, er ansett av mange for å være en viktig komponent i moderne demokratiske rettigheter. Se for eksempel Rouvroy og Poullet (2009).

Standarder for samtykke: fra helseforskning til «digitale krisekart»[4]

Begrepet «samtykke» innebærer generelt at de som gir samtykke gjør det med et minimum av relevant informasjon som muliggjør «informert samtykke». Belmont-rapporten (1979), som omhandlet helseforskning, deler vilkårene for samtykke opp i fem: to som gjelder anvendelse, og tre som gjelder prosess:

> Samtykke kreves i (i) alle typer forskning (ii) på menneskelige subjekter. For at samtykke kan sies å foreligge må forskningssubjektene (iii) bli gjort kjent med forskningsprosjektets formål, metoder og mulige konsekvenser (inkludert risikoer og skader) og (iv) ha rimelig mulighet til å vurdere egen deltakelse og ha anledning til å stille spørsmål om alle aspekter ved forskningen før de samtykker. (v) Deltagelse i forskningsprosjektet må alltid være frivillig.

Selv om helseforskningsområdet skiller seg fra humanitære kriser, er disse vilkårene også relevante her og representerer et bredt anerkjent begrep som også underbygger forståelsen av samtykke i en humanitær kontekst. Da gjenstår spørsmålet om hvordan denne forståelsen kan anvendes til digital humanitær informasjon.

Det har så langt blitt utviklet noen få retningslinjer som tar utgangspunkt i nye medier og strategier for informasjonsbruk og som prøver å kartlegge ansvarsområder og prosedyrer, men som ikke gir operasjonell veiledning. Eksempelvis har GSMAs *Code of Conduct for Disaster Response* (GSMA 2013) som formål å forbedre koordinering mellom telekommunikasjonsleverandører og humanitære aktører under naturkatastrofer. Dokumentet nevner imidlertid personvern kun én gang, nemlig når det fastslår at informasjonsinnhenting bør foregå i samsvar med nasjonale lover og regelverk. Videre anbefaler dokumentet at SMS-informasjon innhentet fra enkeltindivider og andre typer «personlige data» ikke bør deles med tredjepart uten samtykke. Det gis derimot ingen veiledning med hensyn til hvilke krav som stilles til et «etisk» samtykke eller hvordan samtykke bør innhentes.

Det internasjonale Røde Kors (ICRC) er den av de store humanitære aktørene som har kommet lengst i arbeidet med å utarbeide retningslinjer for bruk av digital kriseinformasjon. ICRCs *Professional Standards for Protection Work* fra 2013 omhandler blant annet regulering av sensitiv informasjon og presenterer 15 standarder for hvordan humanitære aktører kan identifisere og håndtere etiske utfordringer som følger med bruk av humanitære data.[5] Dette er så langt det mest detaljerte og innflytelsesrike

4. Oversatt fra «crowdmapping» på engelsk.

5. Kapittel 6: Managing Sensitive Protection information (Standards and guidelines 36–50).

bidraget fra sektoren.[6] *ICRC Professional Standards for Protection Work* inkluderer to standarder som er spesielt relevante for spørsmål om samtykke, nemlig kravet om risikoanalyser og informert samtykke:

> 40. Beskyttelsesaktører som systematisk setter opp informasjonsinnhenting over internett eller andre media må analysere potensielle risikoer som innhenting, deling eller offentlig fremvisning av informasjonen kan medføre og tilsvarende tilpasse måten informasjon samles, kontrolleres, brukes og deles på (ibid.: 86).

> 48. Beskyttelsesaktører må innarbeide forståelsen av informert samtykke når de etterspør hjelp fra offentligheten eller enkeltmedlemmer av et lokalsamfunn om å spontant sende informasjon gjennom SMS, en åpen internettplattform eller hvilken som helst annen form for kommunikasjon eller når man bruker informasjon som allerede er tilgjengelig på internett (ibid.: 95).

ICRC-retningslinjene dekker en rekke vanskelige temaer på en svært god måte. Likevel er retningslinjene ikke tilstrekkelig tydelige på det operasjonelle nivået. Hvem har for eksempel ansvaret for å sette retningslinjene ut i livet i felt, både på organisasjonsnivå og i forholdet til ansatte? På organisasjonsnivå mangler det ressurser, på individnivå mangler det kapasitet. Sees disse praktiske hindringene i sammenheng med brytningen mellom det etiske ansvaret for informasjonsbeskyttelse og formålet om rask og effektiv nødhjelp, kan man stille spørsmål ved om disse standardiseringsøvelsene bidrar til normsetting – og hvorvidt disse normene er mulige å implementere i praksis.

Nye utfordringer: når, hvem og hvordan skal samtykke gis?

Dagens informasjonsøkologi preges av enkel innsamling, umiddelbar deling og grenseløs gjenbruk av informasjon. I denne virkeligheten er det langt fra enkelt å utrede når samtykke bør innhentes. Denne vurderingen må nødvendigvis baseres på grundige risikoanalyser, hvor potensielle farer ved å samle og bruke informasjonen veies mot muligheten for å anvende den på en hensiktsmessig og effektiv måte. Et eksempel: det etableres et system for SMS-rapportering som skal varsle om og dokumen-

6. Spesielt relevant er kapittel 6, som legger frem en anbefaling om at bare organisasjoner med nødvendig ekspertise og kapasitet bør samle fortrolig informasjon (standard 37); at ansvar for å vurdere risiko ligger hos aktører som søker informasjon og bygger systemer for informasjonsdeling (standarder 39, 40, 46); at mekanismer for informasjonssikkerhet må være til stede *ex ante* (standard 45); at vurdering av informert samtykke er nødvendig for deling av informasjon fra intervjuer og «nettdugnad» (crowdsourcing, standarder 47–48); at individer og grupper bør være informert om hvordan informasjon de supplerer kommer til å bli brukt (standard 49); og for etablering av informasjonssystemer og sikkerhetsprosedyrer (53).

tere angrep mot sivile. Ideen om at samtykke er etisk nødvendig fra et beskyttelsesperspektiv er basert på sannsynligheten for at SMS-rapportene kan sette enkeltpersoner i fare da de bidrar med rapporter eller er rapportert om, og fordi identiteten deres kan spores. Utredning av samtykke i en slik situasjon krever både forståelse av trusselbildet og av hvordan en potensielt truet lokalbefolkning kan få innblikk i og tilgang til rapportene (kan de overvåke SMS-trafikk, og er det samarbeid med telekommunikasjonsleverandører?), samt hva informasjonen kan brukes til av de ulike aktørene. Dyp lokalkjennskap er helt nødvendig for å utrede om samtykke trengs, men er ikke nødvendigvis til stede blant humanitære aktører som utreder situasjonen.

Om man går ut fra at det er mulig å utrede om samtykke er nødvendig, gjenstår det en rekke praktiske spørsmål om hvem som skal gi samtykke og hvordan. Spørsmål om hvem sitt samtykke som skal sikres er sammensatt: I tillegg til de som bidrar direkte med informasjon, må man vurdere om det er behov for samtykke fra parter som bare er indirekte berørt og tredjeparter. I SMS-eksemplet ovenfor betyr det at i tillegg til de som sender inn SMS-rapporter, muligens også må innhente samtykke fra personer det blir referert til i rapporter eller fra grupper og aktører som kan bli utsatt for represalier fra lokale grupper eller myndigheter.

Selv når det er klart at samtykke er etisk nødvendig og hvem som bør gi det, kan det være praktiske og strategiske hindringer for å sikre at dette faktisk skjer på forsvarlig vis. For det første kan det være krevende å identifisere og få kontakt med individer og grupper man ønsker å få samtykke av. Hvis man i det tidligere eksemplet kommer frem til at de som skal sende inn SMS-rapportene dermed blir utsatt for en uakseptabel risiko, kan det hende at selv det å søke samtykke kan innebære den samme risikoen. Spørsmålet blir derfor om det trengs samtykke for å søke samtykke. Når bør avgjørelsen for akseptabel risiko ligge eksklusivt hos de humanitære aktørene? Det kan hende at humanitære aktører som bygger opp et rapporteringssystem ikke har direkte kontakt med andre parter som kan bli beskrevet i rapporter. Har informantene, som ofte også vil være mottakere av nødhjelp, samme tilgang til media som de humanitære aktørene som mottar rapporteringen? Ser informantene det humanitære arbeidet i et positivt lys? De samme spørsmålene kan stilles ved tredjeparter som eventuelt kan få økonomiske eller sikkerhetsvansker etter at informasjon har blitt gitt av andre. For store grupper må det også bestemmes om man skal søke samtykke gjennom representanter for gruppen eller sørge for å nå ut til alle potensielle berørte med informasjon om hva man har til hensikt å gjøre. I en slik situasjon vil det igjen være et spørsmål om samtykke bør gis gjennom aktivt tilsvar, eller kan man anse at samtykke foreligger dersom tilsvar ikke gis?

Ifølge Almon & Farkas (2013: 10) kan disse utfordringene håndteres med godt formulerte retningslinjer for personvern og at informanter kan betraktes å ha gitt samtykke når de har lest disse retningslinjene. Men dette hjelper ikke med spørsmål om når samtykke kreves og av hvem, og heller ikke med håndtering av samtykke fra andre- og tredjeparter. Det er neppe noen enkle svar på disse spørsmålene, som krever aktiv utredning og kunnskap om kontekst og hva slags teknologi som blir anvendt i det spesifikke tilfellet.

Selv når man eventuelt kommer frem til adekvate svar på disse spørsmålene, kan det gjenstå en rekke utfordringer knyttet til den informasjon som eventuelle informanter kan dra på. For at samtykke skal være informert, må de som medvirker gis informasjon om formål og risikoer ved informasjonsinnhentingsprosessen (prosesskriterier ii og iii) som fører oss til et velkjent dilemma: jo mer informasjon om risiko, dess mindre vilje til å delta. Dette er spesielt krevende i en situasjon hvor informanter sannsynligvis må gis innblikk i teknologisk informasjon. Det blir for eksempel vanskelig for en selvbergingsbonde uten formell utdanning eller tilgang til internett å forstå og vurdere sannsynligheten for at en militsgruppe vil få tilgang til en programvare som vil gjøre den i stand til å overvåke mobilnettverk eller identifisere individuelle bidragsytere. En reell vurdering av hvilken risiko deltagelse innebærer (vilkår 4), krever dessuten bred kunnskap om hvordan den politiske og rettslige situasjonen vil endre seg over tid – hvordan vil maktbalansen være om fem år, hvordan vil kravene til datalagring være om ti år? Å gjennomføre slike vurderinger er vanskelig nok for eksperter. For eventuelle informanter uten bred kunnskap er det ikke bare vanskelig, men kan kreve introduksjon til en del muligens skremmende informasjon om hvordan teknologi kan bli brukt. Å presentere informanter med informasjon de trenger til å gi informert samtykke, kan rett og slett senke deres motivasjon til å bidra.

Den sentrale spenningen: normer og praksis

OCHA rapporten *Humanitarianism in the Network Age* anbefaler at det innen 2014 skal etableres en rekke retningslinjer og standarder for etisk bruk av data i humanitært arbeid. Sentral blant disse vil være en «do no harm»-standard for digitalt hjelpearbeid:

> Innen 2014 bør det utvikles «do no harm»-retningslinjer for etisk bruk av nye typer data, inkludert protokoller for å ivareta personvernet og garantere informanters sikkerhet, og utvikle rammeverk for å holde aktører ansvarlig for å følge etiske og tekniske standarder. Det bør sikres at disse adresserer de forskjellige problemstillingene rundt personvern, ansvar og sikkerhet på en tydelig måte (OCHA 2013: 60).

Samtidig understreker rapporten at «[b]ekymring rundt informasjon og data ikke kan bli en begrunnelse for å *unngå* bruk av ny kommunikasjonsteknologi i kriser» (ibid.: 46).

Den grunnleggende problemstillingen for denne artikkelen er spørsmålet om hvordan man skal balansere innsats for å sikre etisk behandling og beskyttelse av humanitær informasjon mot målet om å yte rask og effektiv humanitær bistand. En kvalifisert vurdering av hvorvidt samtykke er nødvendig, med påfølgende innsats for å sikre kvalifisert samtykke, er ressurs- og tidkrevende. Når det er uklart hva som skal til for å sikre samtykke, når behovet for samtykke ikke er på det rene og det er usikkert hvorvidt samtykke vil bli gitt, kan det være vanskelig å *ikke* prioritere hurtighet og effektivitetshensyn.

Dette dilemmaet har vært tydelig i flere humanitære kriser. Dilemmaene rundt bruken av SMS for å lage digitale krisekart («crowdmapping») og koordinere den humanitære responsen i etterkant av jordskjelvet i Haiti i 2010, er forholdsvis godt dokumentert. Over 10 000 SMS-meldinger ble samlet inn og kartlagt av en uformell samling av frivillige, ledet av Patrick Meier og i samarbeid med Fletcher School ved Tufts University, Thomson-Reuters Foundation, InSTEDD, US State Department og andre. SMS-ene ble kartlagt under betegnelsen «Ushahidi 4636»,[7] og ettersom det var stor etterspørsel etter dataene fra forskjellige aktører, inkludert US Marine Corps og US Coast Guard, måtte de frivillige avveie hensyn mellom personvern og ønsket om å handle så fort som mulig. Patrick Meier beskriver dilemmaet slik: «... jo åpnere dataene er, dess mer sannsynlig er det at informasjonen er anvendbar for profesjonelle krisearbeidere, lokale aktører og diasporaen – men farvel personvern» (Meier 2013).

Istedenfor grundig risikoanalyse og utredning av behovet for samtykke med utgangspunkt i den aktuelle situasjonen, tok lederne for Ushahidi kontakt med to vestlige advokater og ba dem om deres mening. Begge advokatene argumenterte for at samtykke var innforstått ettersom individer hadde sendt informasjon på SMS. På grunnlag av dette åpnet Ushahidi de 4636 rapportene de hadde samlet, og argumenterte for begrepet «innforstått samtykke» (ibid.).

Uten å ta stilling til om dette var en riktig avgjørelse eller ei, kan det forestilles at dette representerer et gjennomgående perspektiv blant humanitære aktører. Igjen, som formulert av Patrik Meier:

7. Navnet kommer fra «short code» som SMS-meldinger kunne sendes til i Haiti (4636). Samarbeidet ble aldri formalisert, og websiden hvor Ushahidi-applikasjonen ble satt opp (http://4636.Ushahidi.com) er ikke lenger tilgjengelig. Den uorganiserte måten frivillige ble samlet og koordinert på har blitt beskrevet som motivasjonen til å opprette organisasjonen «Standby Volunteer Task Force». For en detaljert beskrivelse av tiltaket, se National Geographic (2012) og Mission 4636 (2013).

> Jeg vil aldri igjen bruke 24 timer pluss for å diskutere hvorvidt tidssensitive liv-eller-død-SMS-meldinger kan eller ikke kan bli kartlagt på grunn av usikkerhet rundt personvern og beskyttelsesansvar – 24 timer under en søk- og redningsfase vil nesten garantert utgjøre liv eller død (Meier 2013).

Mens dette er et legitimt argument, fjerner det ikke imperativet om å beskytte enkeltindivider så vel som grupper mot fare og skade – også når det gjelder risikoer knyttet til personvern og sikkerhet. Uten konkrete retningslinjer for hvordan man skal kunne identifisere og veie konkurrerende hensyn, vil handlingsalternativet oftest vinne i humanitær bistand. Dessverre er det nettopp på dette nivået at retningslinjer som IRCRs *Professional Standards for Protection Work* kommer til kort. Å kartlegge ansvarsområder og eventuelle risikoer er et viktig første skritt, og det er positivt at dette dokumentet presenterer vurderingskriterier som kan hjelpe humanitære aktører med å vurdere den konkrete konteksten de jobber i. Men uten mer detaljer og veiledning om *hvordan* denne avveiningen skal tas, vil humanitære aktører uten teknologisk ekspertise og retningslinjer og prosedyrer velge rask og effektiv handling.

Konklusjon

Dette bidraget har sett på hvordan samtykke kan forstås og implementeres i en humanitær kontekst preget av digital media og fri flyt av informasjon. Selv om begrepet om samtykke er bredt anerkjent i humanitært arbeid og tett knyttet til det humanitære beskyttelsesansvaret, er det uklart hvordan det kan eller skal implementeres i humanitære kriser. Dagens digitale kommunikasjon kompliserer tradisjonelle tilnærminger til samtykke på strategisk og praktisk plan. Dette krever dyp kunnskap og spesielle kapasiteter som er ikke til stede blant de fleste humanitære aktører. Det krever også utredninger og prosedyrer som kan anses som konkurrerende med det humanitære imperativet om rask og effektiv handling. Det er langt fra klart hvordan disse spenningene skal håndteres. Diskusjonen om etikk og digitale medier har så smått begynte å berøre disse spørsmålene, og utviklingen av humanitære retningslinjer har begynt å gå inn på viktige problemstillinger, men gir ikke den operasjonelle veiledningen som trengs for å utrede og implementere samtykke på bakken.

For utvikling av normer og praksis ser det ut som at samtykkedebatten følger to parallelle spor. I felt gjøres konkrete vurderinger av handlingsalternativ løpende, og oftest uten noen videre vurdering av risiko eller personvern. Samtidig har flere internasjonale organisasjoner tatt innover seg at dette er reelle problemstillinger de må ta stilling til. Ut fra anvendelighet og legitimitetshensyn er det viktig at arbeidet med å utvikle retnings-

linjer og standarder både inkorporerer et nedenfra og et horisontalt perspektiv: hvis slike retningslinjer ikke er utviklet i samarbeid med feltarbeidere, kan de oppleves som lite annet enn byråkratiske snublesteiner og med små sjanser for å bli brukt i nødhjelpssituasjoner på bakken. Samtidig må standardene utvikles med tilstrekkelig teknologisk og etisk kompetanse, noe få hjelpearbeidere besitter. I tillegg er koordinering mellom dataekspertene og hjelpearbeiderne (både profesjonelle og frivillige) sentralt – men det er imidlertid uklart hvordan dette samarbeidet bør ser ut. Det første skrittet er en bredere dialog om disse utfordringene og bedre forståelse for hvordan de (kan) håndteres i nødhjelp i felt.

Litteratur

Almon, Gabriele & Otto Farkas (2013) *Issues and Opportunities for Humanitarian Protection and Accountability in the Digital Age: Working Paper*. World Vision.

GSMA (2013) *Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters*. Tilgjengelig på: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/Towards-a-Code-of-Conduct-SMS-Guidelines.pdf. Lesedato: 13.02.2014.

HAP (2010) *2010 HAP Standard in Accountability and Quality Management*. Tilgjengelig på: http://www.hapinternational.org/. Lesedato: 13.02.2014.

Hosein, Gus & Carly Nyst (2013) *Aiding Surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*. London: Privacy International.

Iacucci, Anahi Ayala (2013) *The Conundrum of Digital Humanitarianism: When the Crowd Does Harm*. Tilgjengelig på: https://crisismapper.wordpress.com/2013/11/15/the-conundrum-of-digital-humanitarianism-when-the-crowd-does-harm/. Lesedato: 13.02.2014.

ICRC (2013) *Professional Standards for Protection Work*. Genève: Den internasjonale Røde Kors-føderasjonen (ICRC).

Meier, Patrick (2013) *Launching: SMS Code of Conduct for Disaster Response*. Tilgjengelig på: http://irevolution.net/2013/02/25/launching-sms-code-of-conduct/. Lesedato 13.02.2014.

Mission 4636 (2013) *Collaborating Organizations and History*. Tilgjengelig på: http://www.mission4636.org/history/. Lesedato 13.02.2014.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1979) *Ethical Principles and Guidelines for the Protection of Human Subjects of Research (The Belmont Report)*. Tilgjengelig på: http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html#xinform. Lesedato: 13.02.2014.

National Geographic (2012) *How Crisis Mapping Saved Lives in Haiti*. Tilgjengelig på: http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/. Lesedato 23.02.2014.

OCHA (2013) *Humanitarianism in the Network Age*. New York: FNs sentrale humanitære samordningsenhet (OCHA).

Rouvroy, Antoinette & Yves Poullet (2009) The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy. I S. Gutwirth, R. Leenes, P. De Hert & Y. Poullet (red.) *Reinventing Data Protection*. Berlin: Springer.

Zeineddine, Inas (2012) *Gamification and Crowdsourcing as Engagement Techniques for Human Rights Organizations* [Masteroppgave]. Göteborg: Göteborgs Universitet.