Elektronisk identitetstyveri

Hva er et identitetstyveri og hvordan kan det motvirkes?

Stig Hornnes

Masteroppgave ved Avdeling for Forvaltningsinformatikk

UNIVERSITETET I OSLO

Vår 2009

Forord

Jeg vil først og fremst takke veilederen min Arild Jansen for å har stilt opp med hjelp og råd til alle mulige tider. En takk må også rettes til Security Valley og Christian Meyer som gjennom identitetstyveriprosjektet har gitt meg både hjelp og inspirasjon i arbeidet med denne oppgaven. Jeg vil også takke Thomas Olsen som har delt noen av sine erfaringer og samtidig diskutert problemer og spørsmål med meg. En takk også til Jon Berge Holden som hjalp meg med tilbakemeldinger på de rettslige delene av oppgaven. Til sist må jeg sende en takk til min fantastiske kjæreste som ikke bare har holdt ut med meg i skriveprosessen men som også har hjulpet med korrekturlesing.

Oslo juni 2009

Stig Hornnes

Sammendrag

Denne masteroppgaven retter søkelyset mot hva et identitetstyveri er, og hvordan dette spesielt i elektronisk kommunikasjon og elektroniske medier truer den enkeltes personlige integritet. For å undersøke dette retter oppgaven først fokuset mot teoretiske definisjoner og forskningsarbeider. Det viser seg imidlertid vanskelig å konkludere i dette spørsmålet ettersom definisjonene er av til dels svært generell karakter. Et par av de mest gjennomarbeidede definisjonene, som også i stor grad oppsummerer totalinntrykket ble derfor valgt ut som utgangspunkt for oppgavens videre kartleggingsarbeid.

For å finne svar må de teoretiske arbeidene undersøkes empirisk. Det blir derfor først foretatt en gjennomgang av gjeldende norsk rett hvor formålet er å se etter rettslige argumenter for å avklare begrepets og fenomenet nærmere innhold. Gjeldende rett gir visse anvisninger, og illustrerer bant annet den nære koplingen det er mellom identitetstyveri og bedrageri. Det finnes likevel ikke noe klart svar i jussen så lenge identitetstyveri ikke foreløpig er en juridisk problemstilling. Oppgavens siste halvdel kommer i form av et sikkerhetsarbeid for å identifisere trusler og tiltak og på den måten avgjøre hva et identitetstyveri er. Truslene kan knyttets til fasene i et identitetstyveri og handler om ulike måter for uberettiget tilegnelse av personopplysinger som muliggjør misbruk av en annens identitet. Trusler og tiltak handler derfor om personopplysningers konfidensialitet og integritet samt autentisering av brukere og personer.

Denne oppgavens bidrag er først og fremst å gi identitetstyveribegrepet et presist innhold. Oppgaven peker også på virkemidler i kampen mot identitetstyveri. Arbeidet som er gjort viser at et identitetstyveri består av flere elementer, og at det som kjennetegner et identitetstyveri er systematisk identitetsforedling som muliggjør gjentatt identitetssvindel. Enkeltstående tilfeller av identitetsmisbruk vil dermed i seg selv ikke representere et identitetstyveri. Virkemidler som kan motvirke identitetstyveri omhandler bruk av sterke mekanismer for identifisering og autentisering der hvor det er behov for dette samt anonym kommunikasjon der hvor identitet ikke er nødvendig. Det er med andre ord behov for bevissthet rundt spørsmål knyttet til når det er behov for identifisering. Tekniske tiltak må støttes gjennom andre organisatoriske og tekniske tiltak.

Figurliste

Tabelliste

1. Innledning

1.1 Aktualitet og bakgrunn

9 april 2001 kunne man lese om Kirsten Arneberg som etter en tur på Oslo City i februar samme år merket at VISA kortet var borte. I løpet av våren det året ble posten hennes omadressert flere ganger og hennes folkeregistrerte adresse ble endret, noe som igjen førte til at en hel del personopplysninger kom på avveie. Ved å bestille informasjon fra banken om hennes finansielle situasjon og bekreftelse på arbeidsforhold fra arbeidsgiver ble det bestilt både nytt VISA kort og flere mastercard med kredittgrenser på opp mot 50 000 kroner hver i hennes navn. Kirsten Arneberg var blitt utsatt for identitetstyveri, i det Dagbladet omtalte som "et krimdrama fra virkeligheten"[1].

Årlig utsettes 10 millioner amerikanere for identitetstyveri, og i følge Datatilsynet kan du og jeg regne med å bli utsatt for dette to til tre ganger i løpet av livet dersom problemet vokser seg like stort i Norge[2]. Ved Canadian Internet Policy and Public Interest Clinic ved universitetet i Ottawa Canada (heretter omtalt CIPPIC) har man i lengre tid jobbet med problemstillinger knyttet til identitetstyveri. Et større forskningsprosjekt ble gjennomført i 2007 og produserte 7 publikasjoner knyttet til ulike aspekter ved fenomenet. Dette arbeidet har vært til stor inspirasjon for et treårig *identitetstyveriprosjekt*[3] i Norge ved Høgskolen i Gjøvik, NorSIS og Security Valley. Prosjektet har medlemmer fra en rekke institusjoner, deriblant Justisdepartementet, politiet, og KRIPOS. Undertegnede har selv vært en del av forprosjektet i forbindelse med denne oppgaven. Samtidig har Justis- og Politidepartementet etter innstilling fra Datakrimutvalget foreslått en egen bestemmelse om identitetskrenkelser i den nye straffeloven. Som jeg skal gå nærmere inn på i kapittel 2 er formålet først og fremst å gjøre det lettere å få domfellelse i saker som omhandler krenkelse av andres identitet. Det er for øvrig usikkert når og om bestemmelsen som er forslått i Odelstingsproposisjon nr. 22 for 2008-2009 blir rettskraftig.

Stadig mer av kommunikasjonen i samfunnet går nå via kanaler på nett. eHandel, offentlige nettbaserte servicekontor, online tipping og nettbaserte sosiale samfunn representerer et lite utvalg

[1] http://62.63.40.20/artikler/ident.htm

[2] http://www.datatilsynet.no/templates/article____1891.aspx

[3] http://www.idtyveri.info/

av mangfoldet elektroniske tjenester som finnes. Elektronisk kommunikasjon medfører utstrakt innsamling og behandling av personopplysninger fordi mange slike tjenester krever at brukeren oppretter en konto for å få tilgang. Økt innsamling og behandling av personopplysninger på nett medfører dermed også økt eksponering av disse for uvedkommende fordi løsninger for elektroniske identitetsforvaltning potensielt kan inneha mange svakheter. Personopplysninger på avveie er derfor blitt et økende problem, spesielt internasjonalt men også nasjonalt. Mange brukere kan ha svært mange brukerkontoer knyttet til sin identitet. Bare i elektronisk kommunikasjon med det offentlige har man lenge måttet forholde seg til at forskjellige departementer og etater har brukt ulike løsninger og at ingen av disse har snakket sammen. Det jobbes derfor på et teknisk plan med en offentlig infrastruktur for elektroniske identiteter som inneholder mekanismer for sikker håndtering og utveksling av identitetsdata i kommunikasjon med det offentlige. Første fase av dette prosjektet har vært å få til MinSide og autentiseringsløsningen MinID som gir hver bruker tilgang til en hel rekke offentlige tjenester ved hjelp av én innlogging. En slik løsning er en forutsetning for at offentlige tjenester som blant annet helsetjenester skal kunne bli tilgjengelig via nett, samtidig som det også er et virkemiddel i kampen for å sikre oss som brukere fra identitetstyveri. Dette er et av momentene som skal vurderes når jeg i kapittel 5 skal se på alternative forebyggende tiltak mot identitetstyveri.

Et av hovedproblemene i arbeidet med arbeidet rundt identitetstyveri har vært mangel på en presis og entydig definisjon. Denne oppgaven søker derfor å bidra til at dette kommer på plass. Videre søker denne oppgaven å identifisere trusler og tiltak knyttet til behandling av personopplysninger med spesielt fokus på lagring og behandling i elektroniske medier.

1.2 Problemstillinger og avgrensninger

Forvaltningsinformatikk handler om å se på konsekvenser og utfordringer ved bruk av IKT både fra en samfunnsvitenskaplig, informatisk og et juridisk ståsted. Jeg skal i denne oppgaven se på elektronisk identitetstyveri og hvordan både det offentlige og det private behandler personopplysninger og forvalter elektroniske identiteter.

De overordnede spørsmålene som behandles handler om innholdet i og bruken av begrepet identitetstyveri samt utfordringer, trusler og tiltak knyttet til samfunnets håndtering av personopplysninger og elektroniske identiteter. Oppgaven har konsentrert seg om tre hovedspørsmål i den forbindelse, hvorav det første av disse er:

1. Hva er et identitetstyveri?

Identitetstyveri er et begrep som benyttes hyppig i saker som omhandler ulike typer misbruk av identitet. Jeg har derfor gjennomgått et sett med definisjoner fra inn- og utland for å kartlegge begrepsbruken. Sentralt står spesielt forskningen gjennomført av CIPPIC og forslaget til ny bestemmelse i §202 i den norske straffeloven om identitetskrenkelse. Jeg har videre tatt for meg et utvalg nettaviser og undersøkt hva media omtaler som identitetstyveri. Identitetstyveri er imidlertid også et rettslig spørsmål. Jeg skal derfor også se hvordan handlinger som ifølge gjennomgangen av definisjonene kan kalles identitetstyveri behandles rettslig.

Oppgavens neste fase handler om hvordan personopplysninger med spesielt fokus på *elektroniske* identiteter kommer på avveie.

2. Hva slags trusler står samfunnet overfor vedrørende sikker håndtering og autentisering av personopplysninger?

Oppgavens andre hovedspørsmål har som formål å utforske identitetstyveri ved å ta utgangspunkt i elektronisk lagring og håndtering av personopplysninger. Utstrakt bruk av elektronisk kommunikasjon og elektronisk handel over internett gjør at samfunnet forvalter elektroniske identiteter i stort omfang som gir tilgang på personopplysinger på mange nivå. Jeg har derfor sett nærmere på ulike løsninger for elektronisk identitetsforvaltning og hvordan disse håndterer sikring av konfidensialitet samt identifisering og autentisering av brukere. Jeg har videre sett på kjente metoder og teknikker som anvendes for å få tilgang til personopplysninger i elektronisk kommunikasjon og i elektroniske medier, og slik forsøkt å identifisere truslene knyttet til sikring av elektroniske identiteter. Svaret på oppgavens andre hovedspørsmål fungerer også som empirisk grunnlag for å komme nærmere en besvarelse av det første hovedspørsmålet, og kommer i form av en prosessbeskrivelse av et identitetstyveri.

Oppgavens siste hovedspørsmål søker å bygge videre på trusselbildet og omhandler mulige *tiltak* som kan forhindre at personopplysninger og elektroniske identiteter kan komme på avveie og kan bli misbrukt.

3. Hvilke tiltak kan motvirke problemer knyttet til identitetstyveri?

To overordnede diskusjoner står sentralt i forbindelse med oppgavens siste hovedspørsmål:

- Kan identitetstyveri best forebygges ved å implementere sterke mekanismer for identifisering og autentisering eller bør man bestrebe løsninger som baserer seg på minst mulig identifisering av enkeltindivid?
- Kan eventuelt sterk autentisering og identifisering kombineres med bruk av personvernøkende teknologi for å sikre brukere av elektronisk kommunikasjon og elektroniske medier tilstrekkelig personvern?

Jeg avgrenser denne oppgaven til å omhandle identitetstyveri knyttet til fysiske reelle personer. Som en del av oppgavens andre og tredje hovedspørsmål kommer jeg til å adressere en rekke personvernspørsmål. Jeg avgrenser imidlertid denne drøftingen fra å omfatte personvernspørsmål som ikke er direkte knyttet til identitetstyveri, da en fullstendig analyse og drøftelse av personvernmessige implikasjoner spesielt omkring tiltak i kapittel 5 går utover denne oppgavens formål og rekkevidde. Den samme avgrensningen gjelder i forhold til de rettslige delene av denne oppgaven, hvor jeg kun forholder meg til gjengivelse av relevante rettskilder uten å gå inn på egen vurdering og tolkning av rettslige spørsmål.

1.3 Metodebruk

Jeg benytter meg av et bredt spekter av metoder innenfor både samfunnsvitenskapen, jussen og informatikken for å besvare oppgavens ulike problemstillinger. Noen av metodene er delvis overlappende.

1.3.1 Informatisk metode

Overordnet tar denne oppgaven form av fasene i et sikkerhetsarbeid. Sikkerhetsarbeidet er en risikoanalyse bestående av: (Jansen & Schartum 2005, side 66)

- *Verdibeskrivelse*: beskrivelse av de verdier som skal sikres
- *Identifisere trusler*: hvilke trusler og farer er knyttet til verdiene som skal sikres
- *Sannsynlighetsvurdering*: hvor sannsynlig er det at truslene inntreffer
- *Konsekvensvurdering*: hva er konsekvensen av de identifiserte truslene
- *Sikringstiltak*: hvilke tiltak kan motvirke de identifiserte truslene

Ettersom et analysearbeid er svært krevende vil mitt arbeid heller ta form av *vurderinger* som ikke er like dyptgående som en analyse ville vært. Verdibeskrivelsen finner sted i kapittel 2, kapittel 3 og helt innledningsvis i kapitel 4 hvor jeg gjenomgår det teoretiske innholdet av begrepet identitetstyveri. Truslene identifiseres i kapittel 4 hvor jeg også analyserer konsekvensene av de identifiserte truslene. Kapittel 5 gjennomgår forslag til sikringstiltak og vurderer i hvilke tilfeller disse er fruktbare å ta i bruk.

1.3.1 Dokumentstudier

Dokumentstudier er en metode for å studere *sekundærdata,* også omtalt foreliggende data i motsetning til primærdata som er egne innsamlede data. Jeg benytter meg av dokumentstudier i sammenheng med de andre metodene oppgaven bygger på, Dette gjelder for kvalitativ metode og terminologisk metode, slik at dokumentstudier er gjennomgående for store deler av oppgaven. Spesielt kapittel 2 baserer seg mye på dokumentstudier, men jeg vil også gjennomgå foreliggende dokumenter i kapittel 4 og 5.

1.3.2 Kvalitativ og kvantitativ metode

Jeg har valgt en blanding av kvalitativ og kvantitativ metode som tilnærming til oppgavens problemstillinger.

Kvalitativt metode kjennetegnes gjerne ved et intensivt opplegg kombinert med usystematisk presentasjon og registrering av funn. (Hellevik 2003, side 111) Fordelen med en slik tilnærming er at man kan gå dypt inn i hvert enkelt tilfelle og dermed oppnå bedre forståelse av et gitt fenomen. På den andre siden har man i motsetning til ved en kvantitativ tilnærming ikke mulighet til å trekke endelige konklusjoner fordi undersøkelsen ikke består av et representativt utvalg. Jeg har benyttet meg av kvalitativ metode i kapittel 2 hvor jeg identifiserer og analyserer termer og begrepsbruk ved hjelp av dokumentstudier. Kildene jeg brukte i dette arbeidet ble valgt fra institusjoner hvor identitetstyveri på en eller annen måte var relevant for deres arbeid, og la vekt på at kildene skulle komme fra ulike fagområder for å sikre en bred gjennomgang. Kildene jeg valgte ut er videre hentet fra både inn- og utland, uten at dette var tilsiktet i utgangspunktet. Jeg har funnet kildene gjennom søk i Google, gjennom samarbeid med identitetstyveriprosjektet og via forskningen til CIPPIC.

Kvantitativ metode kjennetegnes ved systematisk innsamling og registrering av sammenliknbare opplysinger om et større antall enheter. Opplysningene uttrykkes gjerne i form av tall plottet inn i et skjema eller en tabell og utgjør gjerne grunnlaget for statistisk analyse av mønsteret i tallene.

(Hellevik 2003, side 111) Jeg benytter meg av kvantitativ metode i forbindelse med avsnitt 2.3 identitetstyveri i media hvor jeg tar for meg begrepsbruk i fem ulike nettaviser fra starten av 2000-tallet og frem til i dag. Innholdet i artiklene er videre kategorisert i tabeller. Utfyllende om undersøkelsen er å finne i avsnitt 2.3 og i vedlegg 1.

1.3.3 Juridisk metode

Min bruk av juridisk metode består utelukkende av å gjennomgå ulike rettskilder for å kartlegge rettstatus innenfor et gitt området. Rettskildene her består i lovforarbeider, NOU´er, stortingsmeldinger og odelstingsproposisjoner.

1.3.4 Terminologisk metode

I følge Heidi Suonuuti (Språkrådet 2008, side 35) består et terminologiprosjekt av å

1. vurdere behov,
2. bestemme målgruppen og avgrense fagområdet,
3. identifisere begrepene,
4. samle inn og registrere terminologiske data,
5. utarbeide termliste,
6. utarbeide begrepssystem og tegne begrepsdiagram,
7. skrive definisjoner,
8. velge eller danne termer,
9. gå gjennom begrepsdiagrammene.

Jeg anvender deler av den terminologiske metoden. Behovsvurdering og avgrensning av fagområdet finner sted innledningsvis, hvor jeg klargjør behovsgrunnlaget for oppgaven. Jeg går deretter videre med punktene 3 – 6 i kapittel 2 hvor jeg gjennomgår ulike kilder for å identifisere og kartlegge terminologiske data. Avslutningsvis i oppgaven skriver jeg definisjon og velger term.

1.4 Begrepsavklaring

Sentrale begrep denne oppgaven bygger på er: *identitetsforvaltning, identitet, identifisering, autentisering, elektronisk identitet, anonymitet*, *pseudonymitet* og *personvern økende teknologi*. Jeg skal i det følgende avklare hvilken forståelse denne oppgaven legger til grunn for disse begrepene.

1.4.1 Identitetsforvaltning

Identitetsforvaltning betegner identitetsadministrasjon, og handler i vid forstand om å identifisere individer og kontrollere tilgang til ulike resurser. Denne oppgaven bruker begrepet om administrasjon, forvaltning og utstedelse av elektroniske identiteter.
Identitetsforvaltning kan deles inn i tre grunnleggende faser:

Innrulleringsfasen

Innrulleringsfasen er hvor en identitet opprettes og hvor man bestemmer

- grad av sikkerhet for senere autentisering,
- autentiseringsmekanisme,
- identifikator og
- hva brukeren eventuelt skal kunne foreta seg i et system.

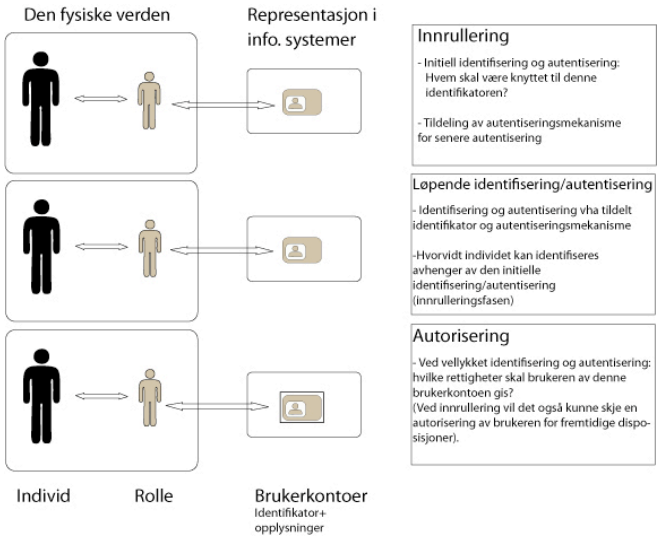
Løpende identifisering og autentisering

Her skiller man mellom to prosesser:

- identifisere: skille brukeren eller individet fra andre,
- autentisere: er brukeren eller individet den de utgir seg for å være.

Autorisering

Dersom den løpende autentiseringen lykkes er spørsmålet videre hva brukeren eller individet skal være autorisert til å foreta seg, enten det er i et datasystem eller i en arbeidssituasjon i den fysiske verden.



Figur 25: Identitetsforvaltningsfaser (NOU 2009:1 , side 286)

1.4.2 Identitet og identifisering

Begrepet *identitet* stammer fra det latinske *idem* som betyr "det samme", og refererer dermed til aspekter ved en person som antas å være konstant. Bokmålsordboka definerer[4] det som følgende:

identite't m1

1 det å være identisk, fullstendig likhet *påvise i- mellom to begreper*

2 sum av element som gir et individ, et samfunn o l individualitet: "jeg"-bevissthet *finne, miste sin i- / nasjonal i- / navn, stilling o l til en person fastslå den dødes i-*

Definisjonen er todelt: nummer 1 definerer det å *identifisere* mens nummer 2 definerer *individualitet*. Identifisering er en formell form av begrepet, og handler eksempelvis om at et identitetsbevis har opplysningene tilhørende den personen som benytter det for å identifisere seg overfor andre. Identifisering er videre å fortelle noen hvem du er: det er prosessen med å skille individer fra hverandre i et et-til-mange forhold ved hjelp av formelle karakteristika. Individualitet på den andre siden handler om den delen av et menneske som definerer en person, eksempelvis aspekter knyttet til et individs følelsesliv.

Identitetsbegrepet kan også omtales med begrepene *prosedural* og *sosialpsykologisk identitet* som har tilnærmet den samme betydningen som identifisering og individualitet. En *prosedural identitet* er en samling av formelle karakteristika egnet for identifikasjon, og er faste karakteristika som følger et individ gjennom hele livsløpet. Den sosialpsykologiske identiteten er det som definerer et menneske, og er i stadig forandring. (Teknologirådet 2005, side 30)

Denne oppgaven legger til grunn en forståelse av identitet som en samling formelle karakteristika egnet for å *identifisere*. Karakteristika egnet for å identifisere omtales som *identifikatorer*. Identifikatorer som identifiserer reelle personer er også *personopplysninger*. Med *identifisering* menes det i denne oppgaven å etablere sikkerhet for hvem en person er i et et-til-mange forhold. (Schartum og Bygrave 2008, side 9)

4 http://www.dokpro.uio.no/perl/ordboksoek/ordbok.cgi?OPP=identitet&bokmaal=S%F8k+i+Bokm%E5lsordboka&ordbok=bokmaal&alfabet=n&renset=j

1.4.3 Autentisering

Begrepet *autentisering* er tett knyttet til *identifisering*. Autentisering er å etablere sikkerhet for at et individ er den han sier han er i et én-til-én forhold. (Schartum og Bygrave 2008, side 9) Autentisering er dermed å bevise at du er den du sier du er. Forskjellige mekanismer kan benyttes til å autentisere et individ: det kan være

- noe du vet, (eksempelvis et passord).
- noe du har, (eksempelvis et fysisk adgangsbevis)
- noe du er, (eksempelvis et biometrisk kjennetegn)
- noe du gjør, (eksempelvis et bevegelsesmønster når man skriver en signatur).

Kombinasjonen av identifikatoren og det du vet/har/er/gjør (autentifikatoren) er autentiseringen.

1.4.4 Elektronisk identitet

En *elektronisk* identitet består av identifikator og autentifikator. Et eksempel er brukernavn og passord. Denne forståelsen av elektronisk identitet er i samsvar med forståelsen man har lagt til grunn i arbeidet med innføring av eID i offentlig sektor. (Justis- og Politidepartementet 2007, side 52)

1.4.5 Pseudonymitet og Anonymitet

En *pseudonym* identitet i elektronisk kommunikasjon er en identitet uten direkte tilknytning til en brukers egentlige identitet, mens å være *anonym* i elektronisk kommunikasjon betyr at det er et totalt fravær av identifiserende identifikatorer. Pseudonymer kan brukes i betydningen av:

- fiktiv
- virtuell identitet

Et pseudonym kan være sterkt eller svakt avhengig av hvor sterk koplingen er til den reelle personen bak. Ved å bruke et pseudonym i elektronisk kommunikasjon kan man fremstå anonymt overfor de man kommuniserer med samtidig som det finnes en kobling til den reelle personen bak.

1.3.6 Personvernøkende teknologi (PETs)

Begrepet personvernøkende teknologi (Privacy Enhancing Technologies – PETS) i snever forstand omhandler organisatoriske og tekniske tiltak for å begrense mulighetene til å identifisere den

enkelte. (NOU 2009:1, side 276) En av de mest siterte definisjonene av PETs er å finne hos Herbert Burkert: "The term privacy-enhancing technologies (PETs) refers to technical and organizational concepts that aim at protecting personal identity." (Burkert, Agre og Rotenberg 1997, side 126) Generelle informasjonssikkerhetstiltak er, selv om disse også vil beskytte identiteter, ikke å regne som PETs etter den tradisjonelle forståelsen av begrepet. Dette er fordi slike tiltak har som formål å sikre innhold og angår derfor ikke muligheten for identifisering direkte. Den tradisjonelle forståelsen har imidlertid vært knyttet til teknologier som har gitt brukere muligheten til å være anonyme eller benytte seg av pseudonym identitet i elektroniske kommunikasjon med andre. Dette er et prinsipielt viktig skille fordi informasjonssikkerhetstiltak er nødvendige men ikke tilstrekkelig for å ivareta personvernet. PETs har derimot fokus på dataminimalitet og å gi brukeren mest mulig kontroll over egen identitet. (Burkert, Agre og Rotenberg 1997, side 125)

Jeg legger til grunn en tradisjonell forståelse av begrepet.

1.5 Oppgavens videre fremstilling

Kapittel 2 redegjør for oppgavens første hovedspørsmål knyttet til begrepsanalyse og begrepsbruk, og består av kvalitative dokumentstudier, terminologisk metode og et mindre kvantitativt undersøkelsesopplegg. Kapittel 3 redegjør for gjeldende rett knyttet til de definisjoner oppgaven velger å gå videre med fra kapittel 2. Kapittel 4 identifiserer trusler knyttet til identitetsforvaltning, mens kapittel 5 tar for seg tiltak for å motvirke identitetstyveri. Avslutning og en kort oppsummering presenteres til sist, hvor jeg på bakgrunn av både den teoretiske og den empiriske gjennomgangen og analysen presenterer forslag til definisjon av og valg av begrep.

Kapittel 2. Litteraturgjennomgang og begrepsanalyse

2.1 Innledning

Kapittel 2 handler om *begrepet* identitetstyveri, hvordan relevante institusjoner bruker dette, og hva de legger av innhold i det. Således er dette kapittelet en teoretisk analyse av begrepsbruk. Det jeg ønsker å få klarhet i er om det finnes én omforent definisjon, eller om det på bakgrunn av definisjonene er mulig å trekke ut en felles forståelse om hva et identitetstyveri er.

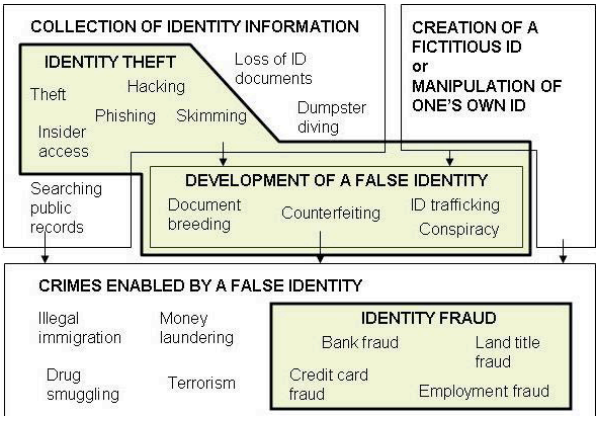
Som en del av kapittel 2 skal jeg gjennomgå forslaget til ny bestemmelse om identitetskrenkelse i straffeloven. Jeg behandler denne på linje med andre definisjoner og ikke som en rettskilde da bestemmelsen ikke har trådt i kraft.

2.2 Gjennomgang av relevante definisjoner

I 2007 gjennomførte CIPPIC et større forskningsprosjekt knytet til identitetstyveri. CIPPIC valgte da å splitte begrepet i *identitetstyveri* og *identitetssvindel*. (Sproule & Archer 2007, side 8)

Med identitetstyveri menes
"The unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information for the purpose of committing fraud or other crimes that involve the use of a false identity."

Med identitetssvindel menes
"The gaining of money, goods, services, other benefits, or the avoidance of obligations, through the use of a false identity."



Figur 26: Modell for identitetstyveri (CIPPIC 2007a, side 2)

Modellen vist i figur 2 er en oversikt over hva CIPPIC mener er identitetstyveri og hva som faller utenfor definisjonens rekkevidde. Identitetstyveri består ifølge CIPPIC av innsamling av personlig informasjon tilhørende en reell person samt utvikling av en falsk identitet med utgangspunkt i personlig informasjon tilhørende en reell person. Identitetssvindel skjer både ved å bruke en reell persons personlige informasjon og også ved å bruke en oppdiktet identitet. CIPPIC valgte en slik fremgangsmåte av hensyn til organisasjonssektoren, og da spesielt bank og finans, som også må ta hensyn til misbruk av oppdiktede identiteter i deres daglige virke.

Datatilsynet definerte sommeren 2007 identitetstyveri som alle situasjoner *"(...) hvor en person, uten samtykke fra rette vedkommende, enten:*

- *helt eller delvis er i stand til utføre en eller annen form for uønsket transaksjon i annen persons navn, eller*
- *skaffer seg tilgang til ressurser tilhørende andre, eller*
- *urettmessig tilegner seg rettigheter som tilhører andre*

vil være identitetstyveri." Tilsynet la seg bevisst på en vid definisjon, selv om de erkjente at den verken var særlig presis eller entydig. (Datatilsynet 2009, side 19) I definisjonen ligger det at det må foreligge en eller annen vinning for gjerningsmannen. Vinningen ser ikke ut til å trenge å være av ren økonomisk karakter, men det må være i form av noe som denne personen ikke ville fått tilgang til med sin reelle identitet. Definisjonen sier videre at det er tilstrekkelig å være i besittelse

av en annens identitet for at det skal kunne kalles et identitetstyveri. Tilsynet gikk videre med å presentere definisjonene identitetstyveriprosjektet har lagt seg på[5]. (Datatilsynet 2009, side 19)

Identitetstyveri

- *Innsamling, besittelse, overføring, reproduksjon eller annen manipulering av annen persons personlige informasjon med den hensikt å skade andres omdømme, begå svindel eller annen kriminell handling.*

Identitetssvindel

- *Ervervelse av penger, varer, tjenester og andre fordeler eller unngåelse av forpliktelser gjennom bruk av falsk identitet .*

Definisjonene fra identitetstyveriprosjektet bygger i all hovedsak på arbeidet til CIPPIC, og er ment som et utgangspunkt snarere enn endelig. Definisjonene fra Datatilsynet ble presentert i en rapport på bestilling fra Fornyings- og Administrasjonsdepartementet. I hovedsak omhandlet rapporten tiltak for å hjelpe ofre som ble utsatt for identitetstyveri, og tiltak rettet mot forebygging, og var basert på en liknende amerikansk rapport fra The President's Identity Theft Task Force (heretter omtalt PTF). Forsamlingen bestående av høytstående amerikanske politikere og embetsmenn definerer identitetstyveri som *"the misuse of another individual's personal information to commit fraud"*, (The President's Task Force on Identity Theft 2007, side 2) og identifiserte tre stadier i et identitetstyveri[6].

- Uberettiget tilegnelse av personlig informasjon,
- forsøk på misbruk av tilegnet informasjon og
- høste avkastningen av svindelen.

Gruppen identifiserte videre fire nøkkelområder samfunnet måtte forbedre for å bekjempe identitetstyveri:

- bedre sikring av sensitive personopplysninger,

[5] Datatilsynet er en av aktørene i prosjektet.

[6] Egne oversettinger av: i) attempts to acquire a victim's personal information, ii) attempts to misuse the information he has acquired, iii) enjoying the benefits.

- bedre autentisering slik at misbruk blir vanskeligere,
- bedre assistanse av ofre og
- mer aggressiv rettsforfølgelse.

Federal Trade Commission[7] (FTC), den amerikanske versjonen av konkurransetilsynet, og US Department of Justice er to andre amerikanske institusjoner som jobber med problemstillinger knyttet til identitetstyveri. FTC definerer identitetstyveri som "*Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes*.", mens U.S Departement of Justice mener identitetstyveri er "*Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain*."[8]. Den amerikanske *Identity Theft and Assumption Deterrence Act* fra 1998 representerer det første legislative arbeidet rundt identitetstyveri, og definerer identitetstyveri som *"(7) knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law:"*. Identity Theft Resource Center[9] (ITRC) er en amerikansk NGO (Non Governmental Organization) som fungerer som en ressurs for ofre og potensielle ofre. Deres definisjon er *"ID Theft is a crime in which the imposter obtains key pieces of information such as Social Security and driver's license numbers. IDENTITY THEFT is when they then use this information for their own gain"*.

FTC knytter identitetstyveri til misbruk av personopplysninger mens U.S Departement of Justice og ITRC også setter det i sammenheng med innsamling. Identity Theft and Assumption Deterrence Act setter heller ikke definisjonen i sammenheng med innsamling av personopplysninger. Grunnen til dette kan være at dette er en rettsregel og at innsamling er regulert på andre måter i amerikansk rett. Alle definisjonene fra amerikansk litteratur knytter seg til reelle personer og ikke fiktive eller virtuelle identiteter.

[7] http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

[8] http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

[9] http://www.idtheftcenter.org/index.html

Home Office Identity Fraud Steering Committee[10] og CIFAS[11] (Credit Industry Fraud Avoidance System) er institusjoner i Storbritannia som blant annet jobber med problemstillinger knyttet til identitetstyveri. Home Office Identity Fraud Steering Committee er resultatet av et samarbeid mellom finansinstitusjoner og det offentlige mens CIFAS er en ikke-kommersiell privat organisasjon bestående av aktører fra det britiske næringsliv. Deres definisjoner av identitetstyveri omfatter:

- ***Identity Theft*** *occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead.*
- ***Identity Fraud*** *occurs when a False Identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud."* (Home Office Identity Fraud Steering Committee)

og

- ***Identity Theft*** *- is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name.*
- ***Identity Fraud*** *- is the use of a misappropriated identity in criminal activity, to obtain goods or services by deception. This usually involves the use of stolen or forged identity documents such as a passport or driving licence.* (CIFAS)

I Storbritannia er identitetstyveri og identitetssvindel innarbeidet som to separate begrep. Et identitetstyveri kan kun innbefatte reelle identiteter mens identitetssvindel også kan forekomme ved bruk av falske identiteter. (Sproule & Archer 2007, side 4)

Finansnæringens Hovedorganisasjon (FNH) representerer bank- og forsikringsbransjen i Norge, og skrev høsten 2008 en rapport knyttet til utfordringer med det de kalte identitetsmisbruk. Rapporten definerte identitetsmisbruk som knyttet til misbruk av forfalsket, fiktiv eller stjålet identitet.

[10] http://www.identity-theft.org.uk/index-2.html

[11] http://www.cifas.org.uk/default.asp?edit_id=561-56

Identitetstyveri ifølge FNH er en type av identitetsmisbruk knyttet til reelle personer og defineres som:

"Dette er forhold der ett individ urettmessig kopierer en reell persons personalia, eller gjennom forfalskede dokumenter klarer å utgi seg for å være en bemyndiget representant for et firma og gjennomfører handlinger (ofte bedragerier) i vedkommendes eller firmaets navn."
(Finansnæringens Hovedorganisasjon 2008, side 5)

Rapporten fra FNH sier at alle problemstillinger rettet mot utstedelse, bruk, verifisering og kontroll av identitetsdokumenter er av interesse for identitetsproblematikken. Spesielt retter rapporten seg mot det offentliges ansvar for utstedelse av godkjente identitetspapir, og peker på hvordan svake rutiner ved innrullering i blant annet folkeregisteret eller utstedelse av pass vil forplante seg i samfunnet fordi slike identitetspapir danner grunnlaget for utstedelse av andre typer ID-kort. FNH peker videre på verifikasjon og kontroll som et av hovedproblemene knyttet til identitetstyveri.

Teknologirådet berører emnet identitetstyveri i en rapport fra 2005 om Elektroniske spor og Personvern, og definerer det som situasjoner *"hvor personopplysninger utnyttes til økonomisk vinning gjennom kredittkortsvindel, låneopptak i offerets navn eller lignende misbruk av offerets identitet"*. (Teknologirådet 2005, side 35) Rapporten fra Teknologirådet omhandler personvern i elektroniske medier og fokuserer på mengden av elektroniske spor vi etterlater oss i hverdagen. Økt bruk av elektroniske medier har medført et nytt kriminalitetsbilde hvor ulike typer datakriminalitet over internett er i sterk økning. Internett har i stor grad også forandret situasjonen for personvernet fordi mulighetene for å spore den enkeltes handlinger samt kartlegge preferanser og forbruksvaner er enkelt tilstede i teknologien. Faren for personvernet er dersom elektroniske spor kan knyttes til enkeltpersoner, og Teknologirådet ser derfor anledningen til å være anonym i elektronisk kommunikasjon som en viktig forutsetning for å ivareta personvernhensyn og dermed redusere mulighetene for å bli utsatt for identitetstyveri.

Datakrimutvalget leverte i 2007 sin innstilling om lovtiltak mot datakriminalitet, og skrev at identitetsmisbruk innebærer *"at noen på en eller annen måte urettmessig benytter en annens identitet"*. (NOU 2007:2, side 33) Utvalget slo fast at dette ofte ble betegnet som identitetstyveri, og gikk deretter videre med å kategorisere økonomisk og annet identitetstyveri. Økonomisk identitetstyveri eksemplifiserte utvalget med at man benytter falsk legitimasjon i skranken i banken i forbindelse med uttak fra en annens konto, eller urettmessig belastning av en annens konto ved

handel på internett. Annet identitetstyveri var ment å fange opp tilfeller hvor misbruk av annens identitet ikke var økonomisk motivert. Utvalget la til grunn at også bruk av falsk identitet skulle regnes som identitetstyveri. (NOU 2007:2, side 34) I følge utvalget er eksempler på identitetstyveri:

- Bruk av falsk legitimasjon ved skranken i banken i forbindelse med uttak fra en annens konto, eller urettmessig belastning av en annens konto ved handel på internett.
- Uttak av penger i minibank ved hjelp av falskt eller stjålet bankkort.
- Sende ut e-post, tekstmeldinger, post eller lignende som utgir seg for å komme fra en annen enn avsenderen.
- Identitetstyveri av juridiske entiteter gjennom phishing[12].

Utvalget gikk deretter videre og foreslo en egen bestemmelse som skulle regulere identitetstyveri. Bestemmelsens første ledd lyder:

"For identitetstyveri straffes den som uberettiget bruker uriktig identitet ved elektronisk kommunikasjon. Som uriktig identitet anses identiteten til en annen fysisk eller juridisk person og identitet som ikke tilhører noen." (NOU 2007:2, side 167)

Forslaget gjaldt bare for elektronisk kommunikasjon og var ment å fremme tilliten til elektronisk samhandling samtidig som det skulle styrke personvernet gjennom å ramme krenkelser av den personlige integritet. (NOU 2007:2, side 90) Ifølge utvalget er identitetstyveri knyttet til bruk av stjålet identitet og bruk av fiktiv identitet. Bruk av stjålet identitet medfører en krenkelse av den personlige integritet mens bruk av fiktiv identitet rammer den som blir ledet til villfarelse, for eksempel en finansinstitusjon som låner ut penger de aldri vil få igjen. Utvalget ønsket at begge skulle omfattes, samtidig som de la vekt på at vanlig bruk av pseudonymer i elektronisk kommunikasjon ikke var ment rammet av bestemmelsen. Datakrimutvalgets forslag dannet grunnlaget for Odelstingsproposisjon 22 2008-2009, heretter kalt proposisjonen, hvor Justisdepartementet videreførte utvalgets forslag til å innføre en egen bestemmelse om

[12] Phishing er en betegnelse på digital snoking eller fisking etter sensitiv informasjon, og brukes som samlebetegnelse på en rekke forskjellige verktøy og metoder for å få tak i dette. Mer om dette i kapittel 4.

identitetstyveri. Jeg skal nå se nærmere på hvordan departementet trekker grensene for hva de mener et identitetstyveri skal være i en rettslig setting.

2.2.1 Ot.prp. 22 § 202 Identitetskrenkelse

Proposisjonen er den siste delproposisjonen i det omfattende arbeidet med å endre straffeloven. Første del av arbeidet resulterte i straffeloven 2005 som inneholder kapitler om alminnelige bestemmelser og straffbare handlinger. Loven er ikke trådt i kraft enda, med unntak av kapittel 16 som regulerer folkemord, forbrytelser mot menneskeheten og krigsforbrytelser. Det er foreløpig ukjent når loven trer i kraft. Det følgende tar utgangspunkt i proposisjonens kapittel 2.9 og 16.2.

§ 202 Identitetskrenkelse

Med bot eller fengsel inntil 2 år straffes den som uberettiget setter seg i besittelse av en annens identitetsbevis, eller opptrer med en annens identitet eller med en identitet som er lett å forveksle med en annens identitet, med forsett om å

a) oppnå en uberettiget vinning for seg eller en annen, eller
b) påføre en annen tap eller ulempe.

2.2.1.1 Departementets identitetsbegrep

Departementet mener at forståelsen av hva en identitet er må bero på en totalvurdering der også sammenhengen opplysningen opptrer i vil ha betydning. ”Navn, fødselsnummer, organisasjonsnummer, webadresser eller lignende vil måtte regnes som «identitet».” ifølge departementet. (Ot.prp. nr 22 for 2008-2009, side 402) Departementet presiserer imidlertid også at ”Det avgjørende må være om den fornærmede lar seg identifisere ved hjelp av midlet som benyttes eller om webadressen eller nettsiden lett kan forveksles med den fornærmedes webadresse eller nettside.”. (Ot.prp. nr 22 for 2008-2009, side 46) Departementet legger dermed til grunn samme forståelse av identitetsbegrepet som denne oppgaven gjør i avsnitt 1.4.2. Dette må imidlertid holdes adskilt fra det departementet kaller *identitetsbevis*, som etter definisjonen i forslaget til ny bestemmelse i § 366 er et utstedt papirbasert eller elektronisk legitimasjonsbevis. Eksempelvis et bankkort eller et digitalt sertifikat. Et identitetsbevis er en identitet, men en identitet trenger ikke være et identitetsbevis.

2.2.1.2 Krenkelse vs. tyveri

Det er interessant å bemerke seg at departementet går bort fra det allmenn kjente og mest brukte begrepet identitetstyveri. Det blir ikke oppgitt noen særlig grunn til dette, men sannsynligvis henger dette sammen med hvordan begrepet *tyveri* benyttes ellers i straffeloven. Straffeloven av 1902 § 257 inneholder legaldefinisjonen av et tyveri: "For tyveri straffes den som borttar eller medvirker til å bortta en gjenstand som helt eller delvis tilhører en annen, i hensikt å skaffe seg eller andre en uberettiget vinning ved tilegnelsen av gjenstanden."

Bestemmelsen forutsetter borttagning av gjenstand i vinnings hensikt. Legaldefinisjonen av løsøregjenstand i § 6 omfatter både tradisjonelle gjenstander i form av fysiske objekter og ulike former for energi ("enhver til Frembringelse af Lys, Varme eller Bevægelse fremstillet eller oppbevaret Kraft.", straffeloven 1902 § 6, jf. utkastet til § 12 i straffeloven 2005: . Iflg. forarbeidene er det ikke tilsiktet materielle endringer ved omformuleringen[13]). I sin utredning om datakriminalitet skriver Datakrimutvalget nærmere om tyveri i forhold til data: "For så vidt gjelder tyveribestemmelsen skaper vilkåret «borttar» problemer, siden «datatyveri» typisk skjer ved kopiering eller overføring av data. Disse handlingene fordrer ikke at de originale data forflyttes. Man kan si at vilkåret «borttar» ikke er oppfylt, eller at begrepet «gjenstand » slik det benyttes i straffeloven § 257 ikke omfatter data." (NOU 2007:2, side 71) Departementet illustrerer dette med Oslo Tingretts dom 10 mars 2005 (TOSLO2004- 84792) da en direktør i et telemarketing selskap ikke kunne dømmes for tyveri da han overførte og kopierte flere tusen datafiler til sin private e-post rett før han meldte overgang til et konkurrerende selskap. (NOU 2007:2, side 70). Forutsetningen for at et tyveri har funnet sted er altså borttagningen av en fysisk gjenstand. Å uberettiget sette seg i besittelse av en annens identitetsbevis vil kunne være tyveri dersom det er snakk om et fysisk identitetsbevis. Bestemmelsen omhandler derimot forhold som ikke vil kunne være i samsvar med legaldefinisjonen av tyveri, som det å opptre med en annens identitet eller med en identitet som er lett å forveksle med en annens identitet. Det vil derfor kunne være rimelig å anta at dette er et sentralt moment departementet har måttet ta hensyn til når man har valgt å ikke bruke tyveribegrepet.

Departementet ser på misbruk av en annens identitet ikke bare som en måte å selv oppnå en vinning (bokstav a), men også i form av å påføre andre mennesker tap eller ulempe (bokstav b). Å påføre

[13] Dette er forelått endre til bare *gjenstand* i den nye straffeloven, men ellers med samme innhold. Se Ot.prp. 90 2003-2004 side 409.

andre en ulempe kan ifølge departementet være å "for eksempel skade fornærmedes gode navn og rykte." (Ot.prp. nr 22 for 2008-2009, side 402) Samtidig som dette igjen tilsier at tyveribegrepet ikke er egnet er dette også et moment som taler for at man har valgt begrepet *krenkelse*. Krenkelse slik det er brukt andre steder i straffeloven er nemlig knyttet til nettopp det å skade en persons gode navn og rykte gjennom bestemmelsene om ærekrenkelser. Videre mener departementet at misbruk av en annens identitet kan oppleves som *integritetskrenkende* (Ot.prp. nr 22 for 2008-2009, side 45) Hva som legges i begrepet *integritet* sier departementet ingenting om, men det fremkommer av Datakrimutvalgets utredning at det er *den personlige integritet* man her taler om. (NOU 2007: 19, side 90) Dette begrepet har sin bakgrunn i personvernteorien, og da i det som kalles *det integritetsfokuserte personvernet*. Dette fokuset behandler personvern som en rekke *sfærer* vi som individ har rundt oss, og kan derfor også omtales som *sfæreteori*. (Schartum & Bygrave 2004, side 24) Utgangspunktet for teorien er at vi som mennesker er frie og ukrenkelige, og skjelner mellom:

- Territorial integritet
- Kroppslig integritet
- Psykisk integritet
- Kommunikasjonsintegritet
- Informasjonsintegritet

Territorial integritet omhandler andres respekt for våre fysiske områder som eksempelvis hjemmet, og kan derfor sies å omhandle privatlivets fred. Den kroppslige integriteten omhandler andres respekt for kroppen vår, og kan typisk eksemplifiseres ved undersøkelser av kroppens hulrom eller biometrisk prøvetakning. Psykisk integritet er komplisert, men kan delvis føres inn under personvernet. Situasjoner som setter noen i psykologiske tvangssituasjoner eller påfører andre følelsesmessige belastninger kan være et brudd på den psykiske integriteten. Kommunikasjonsintegritet er et spørsmål om personvern i den grad andre ikke har respekt for vår kommunikasjon med andre. Å bryte andres brev eller lytte på telefonsamtaler kan være eksempler på slike integritetsbrudd. Informasjonsintegriteten gjelder spørsmål knyttet til integriteten rundt informasjonen som behandles om oss selv. Grunnleggende for å ivareta informasjonsintegriteten er at det er frivillig å gjøre tilgjengelig eller gi fra seg informasjon om seg selv. (Schartum & Bygrave 2004, side 25) Begrepet *identitetskrenkelse* knyttet opp mot den personlige integritet strekker seg altså langt videre enn man ville kunne gjort det dersom man skulle benyttet seg av begrepet *tyveri,* og knytter dessuten fenomenet også til de mer immaterielle og psykiske sidene ved en person. Å

bruke den personlige integritet som begrunnelse setter dermed også bestemmelsen i sammenheng med bestemmelsen om privatlivets fred. (NOU 1997: 19, side 17)

2.2.1.3 Bestemmelsens rekkevidde

Bestemmelsen i § 202 setter grensene for hva som er en identitetskrenkelse til å være

- krenkelse av identitet tilhørende en reell person eller
- krenkelse av en identitet som er lett å forveksle med en annens identitet.

Bruk av fiktiv identitet som ikke tilhører en reell person omfattes ikke. De som kan bli utsatt for identitetskrenkelse er

- juridiske og
- fysiske personer.

Av lovteksten fremkommer det også at krenkelse av en annens identitet innebærer både

- innsamling, jf. det å ”sette seg i besittelse” av en annens identitetsbevis, og
- etterfølgende bruk, jf. det å ”opptre med” en annens identitet.

Med identitetsbevis menes både papirbaserte og elektroniske. (Ot.prp. nr 22 for 2008-2009, side 46) Vilkårene for å kunne dømmes for identitetskrenkelse etter bestemmelsen er enten

- oppnå en uberettiget vinning for seg eller en annen, eller
- påføre en annen tap eller ulempe

Kravet for å dømmes er forsett, som departementet skriver, ” Dersom en person benytter en annens identitet uten at han har forsett om vinning eller holder det for sikkert eller overveiende sannsynlig at noen vil påføres tap eller ulempe, kan han ikke straffes for identitetskrenkelse.”. (Ot.prp. nr 22 for 2008-2009, side 402) Samtidig står det også videre om forsett at ” Det skal ikke være et vilkår for straffansvar at identitetskrenkelsen rent faktisk har hatt en virkning som nevnt i straffebudet. Det avgjørende er om formålet omfattes av gjerningspersonens forsett.”. (Ot.prp. nr 22 for 2008-2009, side 45) Vilkårene er alternative og vinningen som nevnt i det første alternativet trenger ikke å være

av økonomisk karakter. Dette representerer en realitetsendring fra dagens lovverk, noe som kan illustreres gjennom en sak med tidligere Idol finalist Gaute Ormåsen. Ormåsen fikk opprettet et mobilabonnement i sitt navn av en annen person, og abonnementet ble brukt som et ledd i å få kontakt med unge jenter gjennom forumet på Ormåsen sitt nettsted. Ormåsen anmeldte forholdet og mannen ble siktet for bedrageri. Retten fant det derimot ikke bevist at verken Ormåsen eller teleselskapet var utsatt for tap eller fare for tap av økonomisk karakter[14]. Det andre alternativet er en erkjennelse av at en identitetskrenkelse også kan handle om å påføre andre tap eller ulempe. Krenkelse av en annens fred, eksempelvis gjennom å skade en persons gode navn og rykte vil omfattes av begrepet *ulempe*. (Ot.prp. nr 22 for 22 2008-2009, side 402) Bestemmelsen er videre ment å ramme identitetskrenkelse generelt og forslaget er derfor teknologinøytralt.

Identitetskrenkelse slik forslaget er utformet vil også omfatte handlinger som i dag rammes av andre straffebud. Som departementet skriver, ”Selv om flere handlinger som kan tenkes omfattet av straffebudet om identitetskrenkelse i dag er straffbare som forsøk på andre forbrytelser, er det likevel et behov for bestemmelsen. Identitetskrenkelse kan krenke menneskers integritet og sikkerhet uavhengig av om den rent faktisk fører til videre lovbrudd eller ikke. Det vil også være enklere å bevise identitetskrenkelse enn (forsøk på) den fullbyrdete bedragerihandlingen.” (Ot.prp. nr 22 for 2008-2009, side 44) Det virker dermed som om bestemmelsen er noe som kan benyttes i tillegg til andre bestemmelser og ikke nødvendigvis som erstatning for andre bestemmelser. Det foreslås også en ny bestemmelse i § 366 om misbruk av identifikasjonsbevis. I dette tilfellet presiseres det imidlertid at § 202 og § 366 ikke skal anvendes i konkurrens.

Departementet setter også en rekke avgrensninger for tilfeller som skal falle utenfor bestemmelsens rekkevidde. Det settes blant annet som et kriterium at det er et menneske og ikke en maskin som blir villedet, og eksemplifiserer ”(…) bruk av andres pinkoder(…)” (Ot.prp. 2008-2009, side 44. Se også side 402) som ikke sammenfallende med en identitetskrenkelse. Dette er for øvrig den samme sondringen man finner mellom bedrageri og databedrageri i straffelovens bestemmelse i § 270. Tilfeller som dette skal dermed ikke bedømmes som identitetskrenkelse, bestemmelsene i § 201 om uberettiget befatning med tilgangsdata, dataprogram mv. og § 204 om datainnbrudd er ment å ramme slike tilfeller. (Ot.prp. nr 22 for 2008-2009, side 402) Også den nåværende bestemmelsen i § 270 nummer 2 om databedrageri vil kunne tenkes å ramme slike tilfeller, uten at det er spesifisert fra departementets side. Departementet går ikke mer spesifikt inn på hva konkret som faller utenfor

[14] http://www.kjendis.no/2008/11/10/553490.html

bestemmelsens rekkevidde hva angår automatiserte tjenester, og dermed blir det opp til domstolene å avgjøre grensedragningene.

Det er videre slik at det bare er uberettiget bruk av en annens identitet som rammes. Det betyr at bestemmelsen ikke er til for å beskytte en tredjepart som blir villedet ved at noen for eksempel låner bort et identitetsbevis med viten og vilje. Et vanlig eksempel på slikt som da ikke omfattes er at man låner bort identitetsbevis for å lure ekspeditøren bak kassen i butikken at du er gammel nok til å kjøpe alkohol[15].

2.2.1.4 Virtuelle og fiktive identiteter

Bestemmelsen i § 202 er ikke ment å ramme fiktive identiteter. Dette er i følge departementet identiteter som ikke er ens egen men som heller ikke tilhører noen annen. (Ot.prp. nr 22 for 2008-2009, side 43) Begrunnelsen fra departementet synes å være todelt: for det første er skadepotensialet ved å bruke en identitet som ikke tilhører noen betydelig mindre fordi den ikke rammer en som er rettmessig eier av identiteten. For det andre vises det til at bruk av fiktiv identitet i mange tilfeller er anbefalt i elektronisk kommunikasjon, av hensyn til personvern og sikkerhet. Anbefalingen fra Datakrimutvalget om å også la bruk av fiktiv identitet omfattes ble dermed ikke tatt til følge, men ble heller erstattet av ” identitet som er lett å forveksle med en annens identitet”. Det var da heller ikke Datakrimutvalgets hensikt å la all bruk av fiktive identiteter rammes av bestemmelsen, men departementet valgte å ikke bruke begrepet i det hele tatt for å klargjøre hensikten. Det man derimot ikke tar klart stilling til i diskusjonen rundt slike identiteter er hvorvidt misbruk av fiktive identiteter tilhørende en reell fysisk person på nett skal omfattes av bestemmelsen.

Begrepet virtuell betyr noe som gir seg ut for å være, men som ikke er. (Aarseth 2008) Begrepet er blitt mye brukt om det digitale rom fordi man oppfatter dette som at det ikke er virkelig fordi det ikke eksisterer i fysisk form. Begrepet har vært særlig knyttet til online dataspill som World of Warcraft som er et spillunivers hvor spillerne har en karakter som man langsomt bygger opp. Denne karakteren representerer spilleren i spilluniverset og kan være mer eller mindre anonym i forhold til brukerens reelle identitet. Også i andre fora på internett vil man være representert med virtuelle identiteter på samme måte, eksempelvis er det vanlig å benytte seg av såkalt *nick* i debattforum på

[15] Dette er ikke en identitetskrenkelse slik departementet definerer det, men kan tenkes å rammes av forslaget til § 366 om misbruk av identitetsbevis.

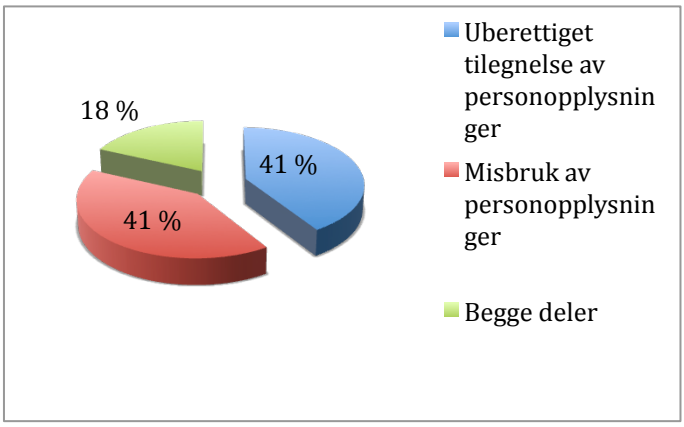
nett. Slik fungerer det for øvrig svært mange steder i forbindelse med sosiale rom og ulike typer nettsamfunn. Virtuelle identiteter hvor man ikke benytter seg av identifiserende personopplysninger vil i prinsippet være det samme som en fiktiv identitet. Slike identiteter er fundamentet for mye av det mer uformelle og sosiale som skjer på internett og er endog anbefalt å bruke spesielt for barn og unge[16]. Det fremkommer også av Stortingsmelding nr. 27 2006-2007 *Eit informasjonssamfunn for alle* at det skal legges til rette for at det også i fremtiden skal være anledning til å opptre anonymt på nettet i de tilfeller hvor det ikke er behov for sikker identifisering. (St.mld. nr. 27 2006-2007, side 139) Det kan derfor ses litt som et paradoks at slike identiteter ikke synes å være tatt med i vurderingen når man har trukket grensene for hva som skal kunne være en identitetskrenkelse. Hvorvidt virtuelle identiteter faktisk blir omfattet eller ikke ser ut til å bero på en konkret vurdering av hvor sterk knytningen til en faktisk person er, eventuelt hvorvidt omverdenen har mulighet til å identifisere den reelle personen bak det fiktive navnet. Når departementet imidlertid omtaler det avgjørende punkt som *identifiserbarhet* synes det klart at koplingen mellom den fiktive identiteten og den reelle personen bak må være klar. Det blir opp til domstolene å avgjøre dette spørsmålet senere.

2.3 Identitetstyveri i norske medier

I dette avsnittet skal jeg ta for meg hvordan media bruker begrepet. Jeg har sett nærmere på saker fra 5 forskjellige nettaviser: VGnett.no, Dagbladet.no, Aftenposten.no, Nettavisen.no og Nordlys.no. Jeg tok for meg 10 saker fra hver av disse ved hjelp av søk i avisenes arkiv på nett, og kategoriserte i hvilke sammenhenger identitetstyveri ble omtalt. Jeg ønsket å se nærmere på to forhold: i hvilken sammenheng ble identitetstyveri brukt, og hvilke handlinger ble da satt i sammenheng med begrepet. Som et fenomen de fleste kun kjenner fra media vil en slik undersøkelse gi en indikasjon på hvordan folk flest oppfatter identitetstyveri. Detaljer, vurderinger og kildeliste ifm. undersøkelsen er å finne i vedlegg 1.

Resultatene i figur 3 viser at like mange artikler omtaler identitetstyveri i sammenheng med uberettiget tilegnelse av personinformasjon, som de gjør det med misbruk. Ikke så mange setter det i sammenheng med begge deler.

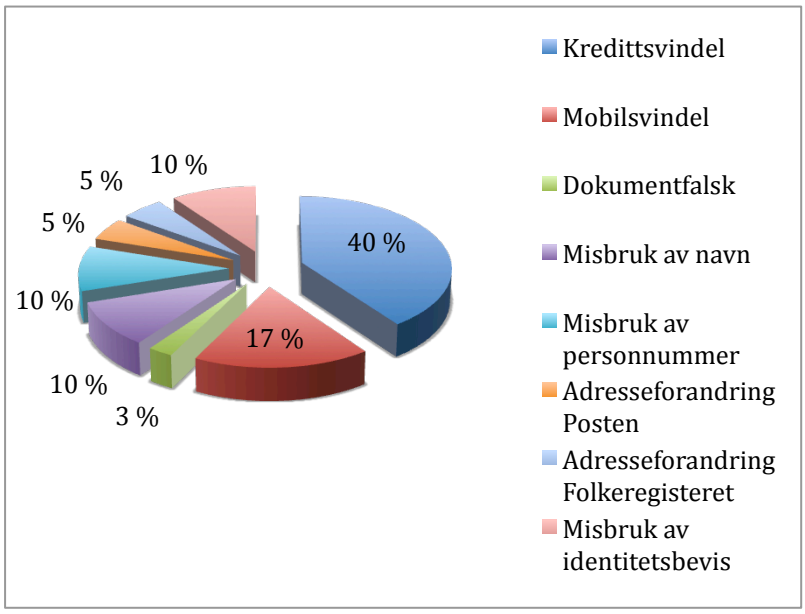
[16] Se www.nettvett.no som er en tjeneste levert av Post- og Teletilsynet.



Figur 27: Identitetstyveri i norske medier

Dette betegner ikke nødvendigvis hvordan de ulike artiklene definerer begrepet, kun i hvilken sammenheng begrepet blir brukt. Det viste seg i gjennomgangen at noen artikler gjorde et forsøk på å forklare fenomenet, slik som Aftenposten gjorde i en sak om lotterisvindel på nett: "I første omgang prøver svindlerne å få tak i informasjon som bankkontonummer, kredittkortnummer, førerkortnummer og passnummer i tillegg til ordinære personopplysninger. Slik kan de drive identitetstyveri og benytte seg av ofrenes kredittkort eller bankkonti." Andre artikler omtalte heller en bestemt hendelse, eksempelvis i en sak hvor skatteetaten feilaktig sendte av gårde 4 millioner personnummer til landets største avisredaksjoner, og satte dette i sammenheng med faren for identitetstyveri. Slike tilfeller, som det var mange av, var ikke nødvendigvis enkle å kategorisere. Jeg landet derimot på at den beste måten å kategorisere var ved å sette det i sammenheng med konteksten artikkelen var skrevet i. Om artikkelen omhandlet personopplysninger på avveie eller lignende og det ikke var presisert i artikkelen at identitetstyveri også var misbruk av disse, ville jeg derfor kategorisere denne som at identitetstyveri er uberettiget tilegnelse av personopplysninger.

Figur 4 viser hvilke handlinger de gjennomgåtte artiklene setter identitetstyveri i sammenheng med.



Figur 28: Ulike typer misbruk av identitet knyttet til identitetstyveri i norske medier

Kredittsvindel er det som klart oftest dukker opp i denne sammenhengen. Kredittsvindel slik jeg har kategorisert det i undersøkelsen omfatter alt som har med misbruk av bankkort, kredittkort eller opptakelse av lån eller kreditt med en annens personopplysninger. Således er denne kategorien også den klart største i omfang. Mobilsvindel omfatter opprettelse av mobilabonnement i andres navn og er også noe som flere ganger har blitt satt i sammenheng med identitetstyveri. Misbruk av navn, identitetsbevis og personnummer er også relativt vanlig omtalte hendelser. Man skulle kanskje tro at misbruk av personnummer ville blitt omtalt oftere, spesielt med tanke på det fokuset personnummeret har fått de siste par årene. Forklaringen på det kan være at i flere av artiklene blir personnummeret omtalt som en sårbar identifikator i forbindelse med uberettiget tilgang til personinformasjon, mens i forbindelse med misbruk av personinformasjon har omtalene vært mindre spesifikke på identitetstyper som blir misbrukt. Omadressering hos posten eller hos folkeregisteret blir bare i beskjeden grad satt i forbindelse med identitetstyveri i de sakene som er gjennomgått. Noen nyanser går imidlertid tapt i en slik undersøkelse, blant annet i forhold til typer av saker. Adresseforandring hos både posten og folkeregisteret har hatt en tendens til å settes i sammenheng med saker om identitetstyveri som også innebærer andre hendelser.

Gjennomgangen av artiklene viser at mediene totalt sett omtaler identitetstyveri som et bredt fenomen, ikke ulikt mange av de definisjonene som er gjennomgått ovenfor. Hver for seg ser artiklene derimot ikke ut til å ha noe formål om å ta for seg identitetstyveri utover det helt overfladiske i sammenheng med misbruk og/eller uberettiget tilgang til personopplysninger.

2.4 Aktører i et identitetstyveri

I følge CIPPIC er det fire aktører involvert i et identitetstyveri. I tillegg kan en femte identifiseres:

1. identitetsholderen,
2. identitetssjekkeren,
3. identitetstilbyderen,
4. tjenestetilbyderen og
5. identitetstyven

Identitetsholderen er den som får sin identitet misbrukt og kan være både en fysisk og juridisk person. En juridisk person er et rettsubjekt med mulighet for å inngå avtaler på samme måten som en fysisk person. Eksempler på slike er stater, institusjoner og bedrifter. Identitetssjekkeren er den som kontrollerer at en person er riktig holder av en identitet. Identitetstilbyderen er den som utsteder en identitet, og tjenestetilbyderen er den som en identitet blir misbrukt hos. Mens identitetsholderen er opptatt av at sin egen identitet ikke skal bli misbrukt vil de tre andre aktørene ifølge CIPPIC også være opptatt av ikke å tilby, autentisere og gi tilgang til ressurser for falske identiteter.

2.5 Begrepsanalyse

Gjennomgangen gjort i dette kapittelet avdekker tre ulike begrep som brukes om hverandre. Dette er

- Identitetstyveri
- Identitetssvindel
- Identitetskrenkelse

Alle begrepene er slik jeg ser det ment å omtale det samme fenomenet, men med ulik merkelapp. Det er videre mulig å se forskjeller i hva som inngår i de enkelte definisjonene. Man kan skille mellom definisjoner som ser på fenomenet som

- uautorisert bruk av personopplysninger
- uautorisert innsamling av personopplysninger
- uautorisert innsamling og bruk av personopplysninger

Det er videre forskjellig syn på hvorvidt både falske og reelle identiteter skal omfattes, og til sist varierer det hvorvidt definisjonene setter opp hensikt/forsett som vilkår. Tabell 1 under kategoriserer hvordan de ulike definisjonene forholder seg til det overnevnte.

	Begrepsbruk			**Innhold i begrepet**		**Identitetstyper**		**Krav om hensikt**	
	ID-tyveri	ID-svindel	ID-krenkelse	Uberettiget innsamling av personopplysninger	Misbruk av personopplysninger	Falsk identitet	Reell identitet	Ja	Ikke definert
Datakrimutvalget	v				v	v	v		v
Teknologirådet	v				v		v		v
Datatilsynet	v				v		v		v
Identitetstyveri-prosjektet	v			v	v	v	v	v	
Ot.prp. 22			v	v	v		v	v	
FNH	v			v	v		v		v
Identity Theft and Assumption Deterrence Act	v			v	v		v	v	
CIPPIC	v			v	v	v	v	v	
FTC	v				v		v		v
PTF	v			v	v		v		v
U.S Department of Justice	v	v		v	v		v		v
ITRC	v			v	v		v		v
Home Office Identity Fraud Steering Committee	v	v		v	v	v	v		v
CIFAS	v	v		v	v	v	v		v

Tabell 1: Begrepsbruk

Debatten om hvorvidt bruk av falske identiteter skal kunne kalles identitetstyveri ble diskutert av Datakrimutvalget og Justisdepartementet i forbindelse med ny straffelov. Som vi ser av tabellen over endte de to på forskjellig resultat. Grunnen fra departementets side var klar: man ønsket å tydeliggjøre at bestemmelsen ikke var ment som en generell kriminalisering av bruk av uriktig identitet. Etter departementets syn var dette uheldig da mye av kommunikasjonen på internett foregår på nettopp denne måten, og bestemmelsen kunne da bidratt til unødvendig usikkerhet knyttet til anonymitet på nettet. Man så videre skadepotensialet som mindre, fordi bruk av falsk

identitet ikke er en identitetskrenkende handling så lenge identiteten ikke tilhører noen. (Ot.prp. nr.22 2008-2009, side 44) CIPPIC gikk motsatt vei fordi man ønsket å ivareta interessene til spesielt bank- og finanssektoren som også blir skadelidende ved bruk av falske identiteter. (Sproule & Archer 2007, side 9) Slike tilfeller er imidlertid dekket av norsk rett gjennom blant annet bedrageribestemmelsen i § 270 (se kapittel 3), og derfor lite hensiktsmessig for Departementet å la være omfattet av bestemmelsen. For å avgjøre hvordan resten av definisjonene forholder seg til falsk og reell eller bare reell identitet måtte jeg vurdere hver enkelt definisjons skriftlige innhold. Definisjoner som benyttet utrykk som knyttet identitetstyveriet til enkeltindivid ble klassifisert som å rette seg mot reelle identiteter. Teknologirådet er et eksempel ved å knytte identitetstyveri til "misbruk av **offerets**[17] identitet". En type falsk identitet som benyttes mye i elektronisk kommunikasjon betegnes virtuell identitet. Slike er gjerne knyttet til sosiale nettsamfunn, og da spesielt i nettbaserte rollespill. En virtuell identitet i denne sammenheng er da en falsk identitet tilhørende en reell person. Det foreligger ingen diskusjoner omkring slike identiteter blant noen av de gjennomgåtte kildene. Datakrimutvalget og Justisdepartementet er innom temaet når de fastslår at det ikke skal være ulovlig å bruke falske identiteter.

Med innføringen av begrepet identitets*krenkelse* kan man si at departementet setter den nye bestemmelsen i § 202 i sammenheng med bestemmelsene om ærekrenkelser og krenkelse av privatlivets fred. Bestemmelsen sikter på å dekke mye av det samme som bedrageribestemmelsen men har et betydelig fokus på ikke-økonomiske og rent injurierende handlinger overfor en annens identitet og har tillegg som mål å gjøre det enklere å få personer dømt for slike handlinger. Rent definisjonsmessig har derimot forslaget mangler fordi bestemmelsen på mange måter fremstår som rettsteknisk. Blant annet innføres det en avgrensning mot maskinell villedning, dvs. brukes det automatiserte midler i gjennomføringen av krenkelsen vil tilfellet falle utenfor bestemmelsens rekkevidde. For allment bruk virker det lite hensiktsmessig å innføre et slikt skille. De andre gjennomgåtte definisjonene viser at det er til dels stor forskjell fra definisjon til definisjon. Spesielt kan man legge merke til at forskjellene er størst mellom landene, selv om denne gjennomgangen i seg selv ikke gir grunnlag for å endelig konkludere. Det synes derfor lite hensiktsmessig å konkludere med hva et identitetstyveri er på grunnlag av teoretiske definisjoner jeg ikke har forutsetninger for å vite hva som ligger til grunn for.

[17] Egen utheving

2.6 Oppsummering og overgang til kapittel 3

På et overordnet nivå synes det å være relativ enighet om hva et identitetstyveri er. Det er imidlertid få aktører som påtar seg oppgaven med å gå begrepet nærmere etter i sømmene, og flere av definisjonene bærer preg av å være svært generelle i sin form. Definisjonene fra CIPPIC og identitetstyveriprosjektet er derimot gjennomarbeidede og dyptgående. Kort oppsummert består deres definisjoner av uautorisert innsamling av personopplysninger (identitetstyveri), utvikling av falsk identitet og etterfølgende misbruk av opplysninger (identitetssvindel) tilhørende

- reelle personer,
- virtuelle identiteter tilhørende reelle personer eller
- juridiske enheter.

Uautorisert innsamling av personopplysninger innebærer innsamling uten identitetsholderens viten eller samtykke. Innsamlingen kan i seg selv være ulovlig dersom metodene som benyttes bryter norsk lov, eksempelvis gjennom ulike metoder for datainnbrudd. Innsamlingen kan være lovlig i den forstand at opplysningene er offentlig tilgjengelig for den som måtte ønske tilgang. Personopplysninger kan også samles inn med samtykke for i etterkant å brukes til et annet formål enn det identitetsholderen opprinnelig samtykket til. Innsamling av personopplysninger tilhørende en annen med den hensikt å bruke personopplysningene til å utgi seg for å være denne vil i seg selv være et identitetstyveri uavhengig av om misbruk finner sted. Identitetssvindel gjennom misbruk av personopplysninger kan skje uavhengig av om et identitetstyveri har forekommet, eksempelvis dersom en verge misbruker identiteten til den han eller hun er verge for.

Et identitetstyveri vil i følge CIPPIC og identitetstyveriprosjektet kunne bestå av handlinger knyttet til

- innsamling,
- besittelse,
- overføring,
- reproduksjon og
- manipulering

av en annen persons personopplysninger. Identitetssvindel er den påfølgende bruken av personinformasjon etter at identitetstyveriet er gjennomført. CIPPIC og identitetstyveriprosjektet mener dette er handlinger knyttet til

- ervervelse av penger, varer, tjenester og andre fordeler,
- eller unngåelse av forpliktelser,
- eller utsette andre for ulemper

gjennom bruk av falsk identitet.

Som utgangspunkt for den videre fremstillingen vil jeg bruke innholdet og forståelsen i definisjonene fra det norske identitetstyveriprosjektet og CIPPIC. Disse definisjonene har en bred tilnærming noe jeg ser som en fordel når oppgaven skal utforske identitetstyveri videre gjennom empiriske undersøkelser. Jeg kommer imidlertid ikke til å gå inn på identitetstyveri av juridiske personer.

Identitetstyveri slik det er definert her består dermed av handlinger som kan tenkes regulert i lovverket på ulike måter. Jeg skal derfor ta med meg beskrivelsene over i kapittel 3 hvor jeg skal se nærmere på hvordan identitetstyveri eventuelt er regulert i norsk rett. Som dette kapittelet allerede har slått fast finnes det ingen egen lovbestemmelse mot identitetstyveri, men som jeg skal illustrere i kapittel 3 finnes det et helt sett med regler som kan knyttes til de handlinger beskrevet over. Kan det tenkes at det finnes rettslige argumenter for utformelsen og forståelsen av begrepet og fenomenet identitetstyveri?

Kapittel 3: Gjeldende norsk rett

3.1 Innledning

Ifølge identitetstyveriprosjektet og CIPPIC består et identitetstyveri av uberettiget innsamling av personopplysninger og etterfølgende misbruk. Det finnes i dag en rekke ulike regler som dekker de ulike handlingene, og da hovedsakelig i hhv. straffeloven og personopplysningsloven. Jeg skal i det følgende se nærmere på aktuelle bestemmelser i lovverket som danner rammen for gjeldende rett, og samtidig vurdere hvorvidt rettslige argumenter kan brukes i forståelsen og utformingen av identitetstyveribegrepet.

3.2 Identitetstyveri

Personopplysningsloven regulerer behandling av personopplysninger, som i § 2 nr. 2 defineres som "enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter". Jeg legger til grunn at alle handlingene beskrevet i avsnitt 2.6 regnes som behandling i lovens forstand.

Innsamling av personopplysninger kan foregå på flere måter:

- På lovlig måte
- På ulovlig måte

Lovlig innsamling av personopplysninger forutsetter at personopplysningsloven ikke overtres[18]. At innsamlingen er ulovlig er da at behandlingen skjer på måter som ikke er anvist i personopplysningsloven, og blir som jeg skal illustrere videre i dette avsnittet regulert gjennom andre regler i lovverket. I praksis innebærer dette situasjoner hvor handlingen bak tilegnelsen i seg selv er gjort ulovlig gjennom bestemmelser i andre lover. Som vi har sett på tidligere blir en persons identitet i stor grad sett på som formelle karakteristika egnet for identifisering. Slike formelle karakteristika knyttet til en person er personopplysninger. Personopplysningsloven regulerer i hvilken grad samfunnet har rett til og i så fall hvordan disse skal behandles. Formålet er "å beskytte

[18] Også annen særlovgivning regulerer personopplysninger, eksempelvis helseregisterloven. Jeg forholder meg kun til personopplysningsloven i denne gjennomgangen.

den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger." jf lovens bestemmelse i § 1. Vi snakker altså ikke om et generelt personvern men et person*opplysningsvern*.

For at behandlingen skal være lovlig stiller lovens §§ 8 og 9 (sensitive personopplysninger) opp visse vilkår som må være tilfredstilt. Dette gjelder krav til samtykke, krav til rettslig grunnlag og krav til nødvendighet. Kravet om nødvendighet utdypes i bokstav a-f i § 8. Bestemmelsen i § 9 har lignende krav. Kravene er alternative, dvs. det er nok at ett av disse er oppfylt. Det stilles videre krav til formålet med behandlingen. § 11 bokstav b setter opp krav om "(…)utrykkelig angitte formål som er saklig begrunnet i behandlingsansvarliges virksomhet,". Å være saklig begrunnet i forhold til virksomheten betyr at behandlingsansvarlige ikke kan starte med behandling av personopplysninger som ligger utenfor bedriftens forretnings- og virksomhetsområde. (Schartum & Bygrave 2004, side 137) Dette kravet skal sikre forutsigbarhet for den registrerte. § 11 bokstav c sier videre at man heller ikke kan bruke opplysningene til et senere formål som er uforenlig med det opprinnelige uten at det foreligger nytt samtykke. Det finnes unntak fra loven dersom behandlingen skjer for rent personlige eller andre private forhold jf. § 3 andre ledd.

Det finnes mange fremgangsmåter for å tilegne seg personinformasjon i henhold til personopplysningsloven. Blant annet gjennom kundeforhold hvor en bruker oppgir informasjon om seg selv i forbindelse med kjøp av en vare over nett. Kunden vil da frivillig avgi opplysninger om seg selv og på den måten oppfyller behandlingen kravet om samtykke i §§ 8 og 9. Dette vil gjelde alle relasjoner hvor en bruker avgir informasjon for å få tilgang til en tjeneste. En annen lovlig måte å tilegne seg personopplysninger på er ved å finne informasjon som allerede er offentlig tilgjengelig i for eksempel offentlige registre eller nettsamfunn som Facebook, dersom formålet med behandlingen er av rent personlige eller andre private formål jf § 3 andre ledd. Om formålet er av en annen karakter vil vilkårene i §§ 8 og eventuelt 9 måtte tilfredsstilles.

Tyveri av post, bankkort eller andre gjenstander som inneholder personinformasjon rammes av straffeloven § 257 og er dermed en ulovlig måte å tilegne seg personinformasjon på. Som vi har sett av tyveridiskusjonen tidligere vil elektronisk informasjon som hovedregel ikke rammes av tyveribestemmelsen, jf avsnitt 2.2.1.2. Det er med andre ord bare tyveriet av det fysiske plastikk-kortet som rammes av bestemmelsen dersom man blir frastjålet bankkortet sitt. Det samme gjelder for tyveri av post, det er tyveriet av den fysiske posten og ikke informasjonen som rammes av bestemmelsen. Straffeloven § 145 første ledd omhandler imidlertid " Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg

adgang til en annens låste gjemmer,". Betegnelsen brev sikter til en lukket forsendelse. Skrift sikter til både maskinskrevet og håndskrevet og kan være notert ned på en hvilken som helst gjenstand. At skriften er lukket innebærer en fysisk forsegling, det holder ikke at et åpent dokument er stemplet fortrolig. Det finnes to måter en overtredelse av straffebudet kan skje på: enten ved å fysisk åpne et brev eller ved å bruke gjennomlysningsutstyr. Begrepet gjemme betyr et oppbevaringssted, dette må være låst. Det innebærer at det er ulovlig å åpne låste skuffer eller skap for å få tilgang til innholdet, for eksempel en låst postkasse for å få tilgang på posten som ligger i den. (Bratholm & Matningsdal 1995, side 214 og 136) Dersom noen stjeler en annens post og tilegner seg innholdet vil man derfor rammes av både §§ 257 og 145.

Handlinger med sikte på å få tilgang til informasjon lagret på elektroniske medier er delvis dekket av straffebud spredt rundt i lovgivningen, og omfatter regler både i straffeloven og åndsverksloven. Justisdepartementet skriver følgende om disse bestemmelsene i siste delproposisjon om endringer i straffeloven: "Uberettiget tilgang straffes etter åndsverkloven § 53 a første ledd og straffeloven 1902 §§ 145 annet ledd og 262 annet ledd, mens tilrettelegging for uberettiget tilgang straffes etter åndsverkloven §§ 53 a annet ledd og 53 c og straffeloven 1902 §§ 145 b og 262 første ledd. Forskjellen mellom disse straffebestemmelsene er at mens åndsverkloven §§ 53 a og 53 c verner åndsverk og straffeloven § 262 beskytter såkalte vernede tjenester, er straffeloven §§ 145 annet ledd og 145 b generelle bestemmelser om straff for henholdsvis spredning av tilgangsdata til «datasystem» og for den som skaffer seg uberettiget adgang til «data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler.» (Ot.prp. nr. 22 2008-2009, side 25) At adgang er uberettiget innebærer at man ikke har en materiell rett til å skaffe seg tilgang, eksempelvis gjennom avtaler, retningslinjer, instruks, arbeidsrettslige regler, regler i kjøps- og avtaleforhold og opphavsrettslige regler m.v. (NOU 2007: 19, side 79) Det er ikke slik at det utelukkende er tekniske tilgangsrettigheter som er avgjørende. Dersom man har tilgangsrettigheter i forbindelse med for eksempel arbeid, og dette opphører, kan det være treghet i systemet som gjør at tilgangen ikke blir fjernet med en gang. Slik tilgang er ikke berettiget. (NOU 2007: 19, side 79) Det finnes grovt sett to måter å begå datainnbrudd på, enten ved å misbruke passord eller ved å utnytte svakheter i et datasystem. Begge deler omfattes av bestemmelsen i § 145 annet ledd.

En annen, og velkjent, måte å samle personopplysninger på er ved å sende ut spam hvor man ber om at mottakeren sender tilbake personinformasjon. Spam er et vidt begrep og omfatter all utsendelse av uønsket e-post. Noen ganger kan det være så harmløst som reklame, andre ganger kan

det være et forsøk på å lure brukere til å sende personinformasjon til seg. Utsendelse av spam er regulert i markedsføringsloven § 2b og gjør det ulovlig å sende uten at mottaker har samtykket på forhånd til å motta det.

Overføring av personopplysninger til andre følger de samme vilkår som for innsamling. Behandling av personopplysninger som er lovlig kan dermed ikke overføres til andre med mindre et av vilkårene i § 8, eventuelt også § 9 dersom det er tale om sensitive opplysninger, er oppfylt. Ved ulovlig overføring av personopplysninger som er lovlig behandlet vil man kunne straffes etter personopplysningsloven. Dersom behandlingen i seg selv var ulovlig vil andre regler kunne komme til anvendelse. Heleri er en form for overføring av personopplysninger tilegnet på ulovlig vis til andre, og er ulovlig etter straffeloven § 317. I motsetning til det som gjelder for tyveri omfatter heleri også informasjon. (NOU 2007: 19, side 74) Heleri omfatter både salg og tilgjengeliggjøring til tredjepersoner. Personinformasjon som er tilegnet på ulovlig vis for å selges til andre, eller for å deles med andre vil dermed også være ulovlig.

Manipulering av personopplysninger kan forekomme som et ledd i et identitetstyveri, og kan omfattes av straffeloven § 291 som egentlig er en bestemmelse som går på skadeverk av gjenstander. I visse tilfeller har man derimot tolket dette vidt slik at uberettiget endring av data også har blitt rammet av bestemmelsen. (NOU 2007: 19, side 71) Som det står videre, ”Tolkningen, som kalles å anvende det «funksjonelle gjenstandsbegrep », ser dataene i sammenheng med det fysiske lagringsmediet som utvilsomt er en gjenstand. På denne måten har man i rettspraksis funnet å kunne anvende straffebudet om skadeverk på «gjenstand » i straffeloven § 291, i saker om uberettiget endring og sletting av data. Det kan blant annet vises til bakdør-kjennelsen i Rt. 2004 side 1619, hvor uberettigete endringer i programoppsettet ble ansett som straffbart etter straffeloven § 291.” Regler om manipulasjon av identitetsbevis finner man også i straffelovens kapittel om dokumentfalsk, jf. neste avsnitt.

Reproduksjon av en annens personlige opplysninger vil kunne være et tema i tilfeller hvor opplysninger lagret på et elektronisk format, i for eksempel et bankkort, blir lest inn på en ekstern innretning[19]. Med riktig utstyr kan man reprodusere disse opplysningene på nye kort et uendelig antall ganger. Gjeldende straffelov har et eget kapitel om dokumentfalsk. Kapitelet inneholder definisjoner (§§ 179 – 181), regler mot bruk (§§ 182 – 184), regler mot selve forfalskningen (§ 185)

[19] Dette kalles skimming, noe jeg kommer tilbake til i kapittel 4.

samt regler mot forberedelse (§ 186). Det er dokumentfalsk både når man endrer et ekte dokument og når hele dokumentet er falskt (Bratholm & Matningsdal 1995, side 405 og 406). Dokumentfalsk handler om å forfalske dokumenter for å utgi seg for å være noen andre, eller for å endre innhold slik at en selv oppnår fordeler eller rettigheter man ikke har krav på. Reglene i § 185 kan ha betydning i forhold til manipulering og reproduksjon av for eksempel identitetsbevis. Det er likevel usikkert hvor langt bestemmelsen kan sies å gå i forhold til identitetstyveri da det som omhandles i bestemmelsen er offentlig protokoll. Det er også uklart i hvilken utstrekning bestemmelsen, og for så vidt også de andre bestemmelsene i kapitelet, er dekkende også for data og databasert informasjon. Ved å bruke det funksjonelle gjenstandsbegrepet kan det tenkes at også dette vil ha et vern, men det er altså uklart. (NOU 2007: 19, side 111)

I sitt forslag til endring av straffeloven 1902 sier departementet i forbindelse med ny bestemmelse i § 202 at man blant annet ønsker ”(…)å utvide straffansvaret slik at bestemmelsen setter straff for den som uberettiget setter seg i besittelse av en annens identitetsbevis(…)”. (Ot.prp nr. 22 for 2008-2009, side 44) Straffeansvaret man her ønsker å utvide ligger i straffeloven 1902 § 372 som regulerer det å opptre med en annens identitetsbevis. Handlingen som gjør en person i stand til å komme i besittelse vil kunne være ulovlig, mens selve besittelsen er antakeligvis ulovlig kun om man rammes av bestemmelsen om heleri i straffeloven 1902 § 317. Denne setter straff for ”Den som mottar eller skaffer seg eller andre del i utbytte av en straffbar handling(…)”.

3.3 Identitetssvindel

Ved å bruke en annens identitet utgir man seg for å være noen andre enn den man virkelig er. Straffelovens § 270 om bedrageri rammer den som i vinnings hensikt forsøker å ”fremkalle, styrke eller utnytte en villfarelse” jf. bestemmelsens første ledd nummer 1. Å utgi seg for å være en annen enn den man virkelig er vil være å skape en villfarelse som er i strid med bestemmelsen. Det er videre et krav om at villfarelsen utløser en handling fra den som blir forledet, som volder tap eller fare for tap for den han handler for. Tapet må være av økonomisk karakter men det er ikke noe krav om at tapet er realisert, derav ”fare for tap”. Dette ble illustrert i den tidligere omtale saken med Gaute Ormåsen. På samme måte tar bestemmelsen i § 270 første ledd nummer 2 for seg databedrageri. Bestemmelsen retter seg mot bruk av uriktig eller ufullstendig opplysning, ved endring i data eller programutrustning eller på annen måte rettsstridig påvirker resultatet av en automatisk databehandling. Kravet om automatisk databehandling innebærer at det ikke er en person men en datamaskin som blir forledet. Misbruk av kredittkort kan illustrere hvordan disse to bestemmelsene fungerer sammen. Databedrageri innebærer at bankkortet er ” benyttet og

«akseptert» direkte av en datamaskin.". Dersom den uberettigede bruken involverer fysisk kontroll av et menneske kommer derimot bestemmelsen i nummer 1 til anvendelse. (NOU 2007: 19, side 110)

Straffeloven § 370 annet ledd tar for seg uberettiget bruk av pass og annet legitimasjonspapir, men henvender seg ikke til identitetsmisbruk generelt. Det kan derimot tenkes at bestemmelsen i § 390 a om krenkelse av privatlivets fred kan ramme slik atferd. (Ot.prp. nr 22 for 2008-2009, side 42) Et annet spørsmål er hvorvidt bestemmelsene i lovens 23de kapittel om ærekrenkelser kan benyttes. Bruk av en annen persons identitet med den hensikt å skade dennes gode navn og rykte vil som vist over ikke kunne dømmes som bedrageri. Bestemmelsen i § 247 sier derimot at "den som i ord eller handling opptrer på en måte som er egnet til å skade en annens gode navn og rykte eller til å utsette ham for hat, ringeakt eller tap av den for hans stilling eller næring fornødne tillit, eller som medvirker dertil kan straffes".

3.4 Betraktninger

Det finnes utfordringer knyttet til det juridiske aspektet ved identitetstyveri. Slik jeg ser det gjelder dette først og fremst å skape et tydeligere regelverk med klarere henvisninger til hvordan identitetstyveri skal reguleres, eller vedta en ny bestemmelse slik Justisdepartementet har foreslått. Slik situasjonen er nå vil det finnes tilfeller hvor det er uklart hvilke regler som skal benyttes, eller om det i det hele tatt finnes regler som er dekkende. Den omtalte saken med Gaute Ormåsen ble behandlet av Lister Tingrett og illustrerer hvor komplisert saker med misbrukt identitet kan være. I et intervju med Dagbladet i etterkant av at gjerningsmannen ble frikjent for forholdet svarte aktor som følger:

"- Burde det ikke i så tilfelle ha blitt tatt ut en annen tiltale, som bedre dekket det aktuelle forholdet?

- Det kan være et tema hva telefonene rent konkret har vært brukt til. En ting er at navnet hans fremstår i dårlig lys, men dette etterforsker ikke politiet. Ærekrenkelser faller inn under privatretten. Men det er klart, i andre saker er det fort gjort at det kommer inn på andre straffebestemmelser. Utifra denne saken, var det mest nærliggende å ta ut tiltale for bedrageri, sier Rue til Dagbladet.no."

- I ettertid kan det jo tenkes at andre paragrafer også kunne vært aktuelle, legger han til."[20]

Dette gir en indikasjon om at regelverket enten ikke er tilstrekkelig eller ikke er oversiktlig nok. Gjennomgangen i dette kapittelet viser at begge antakelsene er nærliggende å anta. Videre er det en utfordring at strafferammene er ulike for de enkelte bestemmelsene i lovverket som omhandler identitetsmisbruk. Dette kan medføre at det blir til dels store sprik i hva man kan bli ilagt av straff. Alternativene man kan se for seg er enten å i) samle regler som går på identitetsmisbruk i egne lovbestemmelser eller ii) å bygge ut eksisterende regler slik at tilfeller som med dagens lovgivning faller utenfor vil bli inkludert. Dette blir imidlertid en rettsdogmatisk diskusjon som går utenfor denne oppgavens rekkevidde og forfatters kompetansenivå å vurdere. Jeg vil nøye meg med å konstantere at departementet har gått for alternativ i).

Det er likevel relevant å spørre hvorvidt man trenger en ny lovbestemmelse så lenge identitetssvindel ligger så tett opp til bedrageribestemmelsen. Er identitetstyveri vesentlig forskjellig fra bedrageri? En hovedforskjell er at det i motsetning til et bedrageri vil kunne være en tredjepart involvert i et identitetstyveri: man har i) den som forleder, ii) den som blir forledet og til sist iii) den som får si identitet misbrukt. Denne egenarten og erkjennelsen av påkjenningen av å vite at noen andre misbruker din identitet kan være et argument for å likevel skulle skille ut identitetstyveri i en egen bestemmelse. I tillegg kan den økte eksponeringen av personopplysninger på nett og den voksende tendensen til at disse kommer på avveie og blir misbrukt være et argument i samme retning, noe jeg kommer mer tilbake til i kapittel 4. Bedrageribestemmelsen omfatter videre kun handlinger som resulterer i økonomisk tap som jeg har illustrert over. Uberettiget tilegnelse av personopplysninger samt rent injurierende handlinger faller utenfor bestemmelsens rekkevidde. Identitetstyveri deler imidlertid mange av de samme egenskapene som et bedrageri all den tid det handler om å fremstå overfor en annen part som noen andre enn den man er. Med utgangspunkt i definisjonene til CIPPIC og identitetstyveriprosjektet synes det likevel klart at bedrageribestemmelsen og dets innhold ikke er helt dekkende slik den står i dag[21].

[20] http://www.kjendis.no/2008/11/10/553490.html

[21] Interessant å bemerke seg er en sak fra Follo Tingrett (saksnr. 08-099861MED-FOLL) hvor retten på side 48 i dommen la vekt på den nye bestemmelsen i § 202 som relevant for utmåling av straff på tross av at den ikke er trådt i kraft enda.

3.5 Konklusjon

Gjeldende rett kan tenkes å bidra til forståelsen og utformingen av identitetstyveribegrepet ved å angi den rettslige tilstanden for de handlinger som identifiseres med et identitetstyveri. For eksempel viser gjennomgangen i dette kapittelet at et identitetstyveri ikke i veldig stor grad viker fra den rettslige forståelsen av et bedrageri. Rettstilstanden og de rettsdogmatiske diskusjonene jeg var inne på i kapittel 2 synliggjør også etter min mening hvordan og hvorfor identitets*tyveri* som begrep er misvisende, jf. avsnitt 2.2.1.2 i forrige kapittel. Kritikken mot begrepet, utover dets vage innhold, har gått nettopp på bruk av begrepet *tyveri*. Når man da fremdeles velger å bruke begrepet uforandret synes det å være fordi begrepet er allment kjent og godt innarbeidet hos folk flest. I hvert fall var dette begrunnelsen hos CIPPIC. (Sproule & Archer 2007, side 2) Kanskje kan man imidlertid si at begrepet oppfattes misvisende fordi innhold er definert såpass vagt og vidt som det er. Analyser av teoretisk definisjoner og rettsregler gir imidlertid ikke svar på dette. Jeg kommer derfor også i fortsettelsen til å bruke identitetstyveri, mens jeg vender tilbake til valg av terminologi i avslutningen.

Kapittel 4: Trusselbildet - Prosessbeskrivelse identitetstyveri

4.1 Innledning

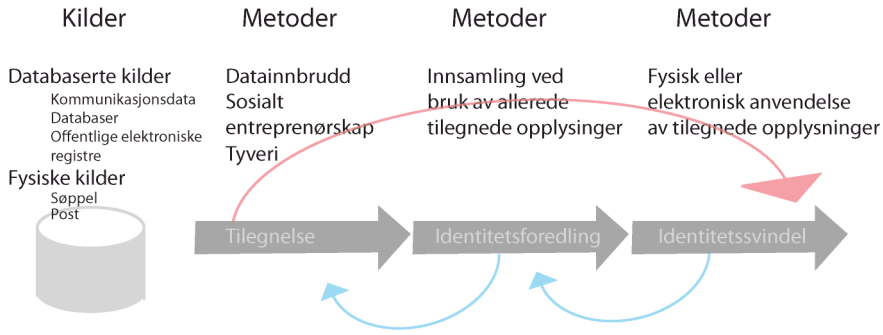
Internett er i løpet av et tiår blitt verdens største medium og sosiale møteplass, og både det private og det offentlige har etter hvert forstått hvilke gevinster man kan få ved å utnytte internetts kapasitet: rask og enkel tilgjengelighet for brukerne og en potensiell effektiviseringsgevinst for dem selv. De siste ti års utvikling hvor majoriteten av i hvert fall den vestlige verden har fått tilgang på pc og internett har ført til at utviklingen av nettbaserte kommunikasjonskanaler, butikker og servicesentre har skutt fart for alvor. I 2006 viste tall fra Statstisk Sentral Byrå (SSB) at 75 prosent av norske husstander hadde PC. 60 prosent av befolkningen brukte internett i løpet av en gjennomsnittsdag men 32 prosent av internettbrukerne brukte nettet til enten privat varekjøp eller nettbank. Så mange som 61 prosent av befolkningen hadde handlet på nett minst én gang siste 12 måneder. (SIFO 2007, side 17-20) For å få tilgang til mange av disse tjenestene er det ofte en forutsetning at man må registrere seg med personopplysninger og opprette elektroniske identiteter. Resultatet er at personopplysninger lagres og behandles i langt større grad enn tidligere.

Også fysiske format inneholder imidlertid personopplysninger, og jeg skal derfor ikke utelukkende fokusere på personopplysninger i elektroniske medier. Selvangivelser, bankkort, diverse pinkoder og tilgangsnøkler til elektroniske identiteter sendes fremdeles via tradisjonell postgang og representerer dermed en minst like stor trussel mot det enkelte individ. Identitetstyveri i elektroniske medier gis likevel et større fokus på grunn av dets potensial. Kapittelet er første del av en sikkerhetsvurdering hvor jeg først beskriver *verdiene* som skal sikres, i dette tilfellet personopplysninger. Jeg går deretter videre med å identifisere *trusler* som kan redusere sikkerheten gjennom uønskede hendelser. Til sist skal jeg gjøre en *risikovurdering* og deretter identifisere *konsekvensene* av truslene. Kapittel 5 fullfører sikkerhetsarbeidet ved å ta for seg tiltak for å motvirke truslene identifisert i dette kapittelet.

4.2 Fasene i et identitetstyveri

I følge CIPPIC består et identitetstyveri av uberettiget innsamling av personopplysninger og misbruk av personopplysninger. (CIPPIC 2007a, side 2) Jeg tror det imidlertid kan være fruktbart å dele et identitetstyveri i tre faser:

1. Tilegnelse av personinformasjon,
2. identitetsforedling og
3. identitetssvindel.



Figur 29: Prosessmodell identitetstyveri

Hver enkelt fase består av ulike metoder som representerer trusler mot den enkeltes identitet og en risiko for identitetstyveri. Figur 5 illustrer hvordan fasene i et identitetstyveri henger sammen, og illustrerer to ulike fremgangsmåter:

- Tilegnelse av personinformasjon med påfølgende identitetssvindel
- Tilegnelse, videreforedling av identitet ved bruk av personopplysninger og deretter identitetssvindel. Prosessen gjentas gjerne flere ganger og kjennetegner identitetstyveri av systematisk og målrettet karakter.

Jeg skal i det følgende ta for meg de ulike fasene og identifisere trusler som kan knyttes til hver enkelt fase.

4.2.1 Tilegnelse av personinformasjon

Truslene i denne fasen knytter seg til metoder og teknikker som utfordrer *konfidensialiteten* og *integriteten* til personopplysninger. Ikke alle personopplysninger har imidlertid *verdi* i en slik sammenheng. Verdien av opplysningene avhenger av hva opplysingene gir *tilgang til*. Et sett med opplysninger med spesielt stor verdi kan identifiseres gjennom at disse i mange tilfeller blir godtatt som autentifikator og dermed gir tilgang til ressurser og tjenester.

- Fødselsnummer
- Passord og Pinkoder

- Elektroniske identiteter
- Førerkort med tilhørende opplysninger
- Kontonummer
- Kredittkortnummer
- Pass/passnummer
- Organisasjonsnummer
- Skatteopplysninger

Flere av opplysningene på denne listen er i utgangspunktet offentlig tilgjengelig informasjon, blant annet er et organisasjonsnummer ment å være offentlig for å skape trygghet for næringslivet. Fødselsnummer er også tilgjengelig for mange dersom det finnes et saklig behov for det, samtidig som det forekommer at fødselsnummeret brukes som autentifikator. For elektroniske tjenester står brukernavn og passord i en særstilling. Alle elektroniske tjenester som tilbyr funksjonalitet mot registrering av personopplysninger regulerer tilgangen med brukernavn og passord.

4.2.2 Identitetsforedling

Identitetsforedling kjennetegnes ved å bruke tidligere tilegnede opplysninger om personer eller brukerkontoer[22] for å få tilgang til mer informasjon, og synes å være en ingrediens ved tilfeller av mer systematisk og målrettet identitetstyveri. For at identitetsforedling skal være mulig må de tilegnede opplysingene kunne gi tilgang til flere opplysninger. Et kredittkortnummer vil eksempelvis kunne brukes for å kjøpe ting via nett i andres navn, men vil ikke i seg selv gi tilgang til andre opplysninger om den rettmessige innehaveren. Andre opplysninger vil derimot kunne tenkes på gi slik tilgang. Trusler i denne fasen knytter seg slik jeg ser det til *autentiseringsmekanismer*: rettigheter blir tilgjengeliggjort for andre enn den rettmessige innehaveren.

4.2.3 Identitetssvindel

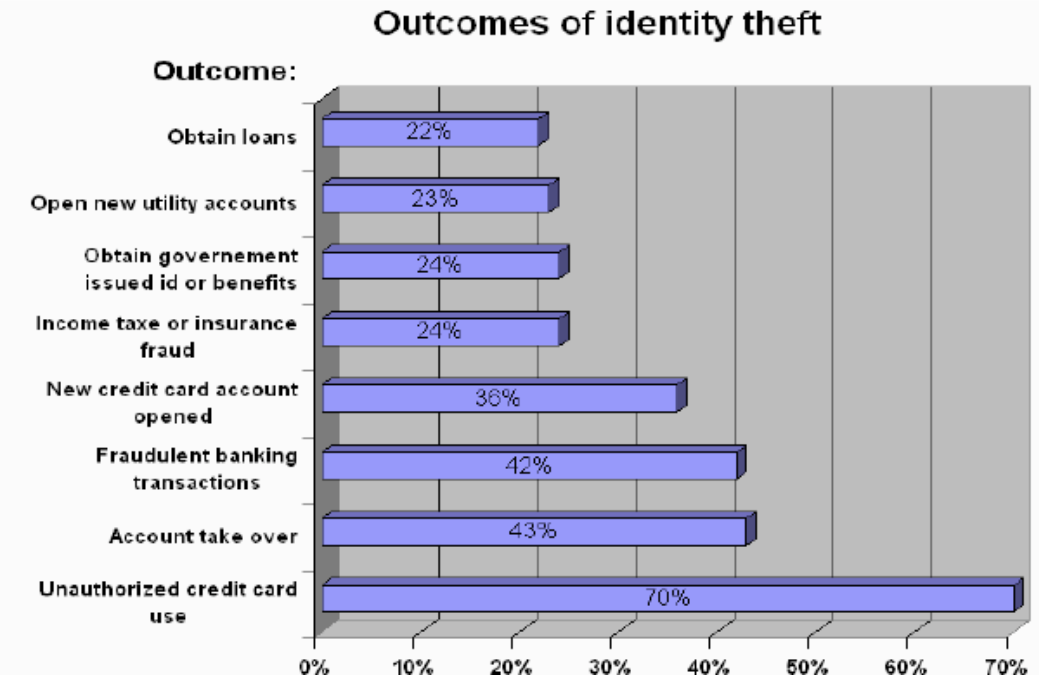
Identitetssvindel er misbruk av tilegnede opplysninger om personer og brukere. I følge CIPPIC (CIPPIC 2007b, side 24-30) kan tilegnede personopplysninger tilhørende andre brukes til blant annet å:

[22] Ved bruk av anonym eller pseudonym identitet vil ikke opplysningene være knyttet til personer men til brukerkontoer.

- opprette kundeforhold
    - netthandel, bank- og forsikringsforbindelse, lån, mobiltelefon.
- utnytte eksisterende kundeforhold
- forfalske identitetsdokumenter
- bestille varer og tjenester on-line
- skaffe seg arbeid
- få utstedt identitetsdokumenter
- få tilgang til helsetjenester og andre offentlige tjenester
- overta e-postkonto
- unngå heftelser på egen identitet.

Identitetssvindel kan dermed sies å ha tre ulike formål: i) man ønsker å oppnå egen vinning, ii) man ønsker å unngå heftelser på egen identitet eller iii) man ønsker å påføre andre skade av økonomisk eller annen art (krenkelse). På samme måten som ved identitetsforedling er truslene her knyttet til *autentisering* av brukere.

En undersøkelse gjennomført i Canada gjengitt av CIPPIC viste hvordan 1001 canadiere svarte når det gjaldt hvordan deres, eller mennesker i dere umiddelbare omkrets, personopplysninger ble misbrukt.



Figur 30: Bruk av personopplysninger til svindel (CIPPIC 2007b, side 23)

Spørsmålet videre er på hvilken måte truslene mot lagrede eller fysiske personopplysninger og autentiseringsmekanismer utløser uønskede hendelser som kan få konsekvenser i form av identitetstyveri.

4.3 Trusler mot personopplysingers konfidensialitet og integritet

4.3.1 Innledning

Jeg vil starte med å se på trusler mot sikring av *konfidensialitet* og *integritet* av personopplysninger i elektronisk kommunikasjon og i elektroniske medier. Som eksempel skal jeg se på to store nettbaserte tjenester som tilbyr brukere funksjonalitet mot registrering av person- eller brukeropplysninger. Med nærmere 200 millioner aktive brukere på verdensbasis[23], og 1,9 millioner registrerte brukere i Norge[24], er Facebook det største sosiale nettverket på internett. CDON.com reklamerer med å være Nordens største underholdningsbutikk på nett, og selger bøker, film, musikk og elektronikk. Disse løsningene er interessante å se på i forhold til tilegnelse av personopplysninger fordi de driver utstrakt innsamling og behandling som igjen fører til økt tilgjengelighet for slike på nett. Tilgjengeliggjøringen kan imidlertid forekomme både fra behandlingsansvarliges[25] side og fra brukerens side fordi opplysninger knyttet til en elektronisk identitet kan lagres begge steder. Facebook og CDON representerer tjenester og tekniske løsninger som er relativt utbredt på nettet, og fungerer dermed som en illustrasjon på spredningen av personopplysinger på nett. Ingen av løsningene behandler i utgangspunktet sensitive personopplysninger, og Facebook *kan* sågar benyttes uten å oppgi reelle opplysninger. Tjenestene er likevel relevante både som ledd i identitetsforedling eller som ledd i et identitetstyveri hvor hensikten er å skade en annens omdømme. Utgangspunktet er knyttet til *hva* tjenestene registrerer om brukeren og *hvordan* denne informasjonen lagres og behandles i begge ender.

Brukerne må både i Facebook og CDON registrere seg med informasjon om minimum navn, e-post, passord, kjønn og fødselsdato. CDON ber i tillegg brukeren oppgi fødselsnummer og i hvilket land vedkommende bor, mens Facebook som et sosialt fenomen også lar brukerne registrere og dele informasjon om seg selv med venner i et nettverk. Derfor er det mulig for å registrere en rekke andre mer trivielle opplysninger samt publisere bilder i et eget fotoalbum. Brukeren regulerer

[23] http://www.facebook.com/advertising/?src=pf

[24] http://www.digi.no/810468/facebook-gir-daarligere-karakterer

[25] Jf. personopplysingsloven § 2 første ledd nummer 4.

imidlertid selv hvem som skal få tilgang på informasjonen. For mange brukere vil det for eksempel være naturlig å lukke profilen for innsyn fra andre enn vennene i nettverket sitt. For andre vil man dermed kun være søkbar med for eksempel navn og profilbilde. Ved kjøp av varer hos CDON må brukeren oppgi kredittkortkortinformasjon, dvs. kortnummer, cvc kode, utløpsdato og navn på kortets innehaver. Man kan derimot også velge å få tilsendt faktura, og da må man i tillegg oppgi det femsifrede personnummeret slik at selskapet har anledning til å foreta kredittsjekk før varen sendes. Opplysninger knyttet til kredittkort lagres ikke, men benyttes kun for å gjennomføre betaling.

I tillegg til opplysninger brukeren frivillig gir fra seg registrerer og logger begge tjenestene opplysninger om type nettleser og IP-adresse på alle som besøker nettstedet. Ved innlogging lagres det innloggings informasjon i informasjonskapsler (cookies) som automatisk slettes når brukeren lukker nettleseren.

Facebook og CDON er bedrifter som lever av å selge informasjon om brukere. Facebook tjener sine penger på annonsører som ser potensialet i ekstremt målrettet markedsføring. Basert på de opplysningene brukerne selv oppgir kan Facebook filtrere annonser. Slik har annonsøren større sannsynlighet for å treffe sin målgruppe samtidig som annonsene blir mest mulig relevante for den som ser dem. På samme måte bruker CDON opplysninger fra brukerne til å markedsføre sine egne produkter overfor kunder og besøkende ved å ha en dynamisk nettside som skal oppfattes ”personlig”. Forretningsmodeller som dette er vanlig for nettbaserte tjenester og gjør det mulig for brukere å få gratis tilgang til mye innhold. Avgivelse av (person)informasjon om brukere til tredjeparter er en del av bruksvilkårene for begge tjenestene og er i så måte frivillig da tjenestene krever at bruker samtykker før tilgang blir gitt. Videre tillater både Facebook og CDON brukerne å lagre sin elektroniske identitet i nettleseren.

I Facebook sine bruksvilkår fremkommer det at selskapet har rett til å beholde arkiverte kopier av brukernes profiler. I tillegg sier bruksvilkårene at brukeren gir Facebook en ” ugjenkallelig, evigvarende, ikke-eksklusiv, overførbar og fullt betalt verdensomspennende lisens (med rett til underlisens) til å bruke, kopiere, offentlig fremføre, offentlig vise, reformatere, oversette, sitere (helt eller delvis) og distribuere slikt Brukerinnhold til et hvilket som helst formål, det være seg kommersiell eller for annonsering eller annet - på eller i forbindelse med Nettstedet eller som markedsføring av det, for å produsere avledede produkter av, eller for å inkludere slikt

Brukerinnhold i annet arbeid, og til å tilby og autorisere underlisenser av det ovennevnte."[26]. Facebook sitter med andre ord på en database med svært verdifulle personopplysninger om nærmere 200 millioner mennesker verden over som de har lisens til å bruke for alltid. Brukere vil dermed være i risikosonen for identitetstyveri også etter at man eventuelt har valgt å avslutte forholdet med tjenesten. CDON har ingen informasjon om hvordan man eventuelt går frem for å slette en brukerkonto, og har heller ingen synlig valg for dette når brukeren er innlogget. Brukeren blir bare henvist til kundeservice dersom man har spørsmål vedrørende retting og innsyn.

4.3.2 Identifiserte trusler

Facebook, CDON og ikke minst brukerne står ovenfor en rekke forskjellige trusler i form av teknikker og metoder som gir uberettiget tilgang på personopplysinger. Truslene kan kategoriseres enten som *sosial manipulering* (social engeneering) eller *datainnbrudd*.

Sosial manipulering er oversatt fra det engelske begrepet social engineering og brukes om det å overtale eller manipulere mennesker til å gjennomføre bestemte handlinger. Sosial manipulering i den form jeg omtaler det som her er rettet mot *brukere* av elektronisk kommunikasjon med det formål å få tak i personopplysninger som kan misbrukes. Jeg skal se på en type sosial manipulering kalt *phishing*. Begrepet kommer fra det engelske ordet *fishing* og brukes om det å fiske etter informasjon. Phishing kan forekomme enten som en mail eller i form av en falsk nettside.

Datainnbrudd kan ramme både brukere og behandlingsansvarlige, og innebærer i følge Datakrimutvalget en "(…)urettmessig tilgang som kan ramme datasystemets innehaver både ved at dataene som er lagret på systemet blir kjent for uvedkommende (konfidensialitet), ved at dataene som er lagret på systemet blir endret urettmessig (integritet) og at systemet som sådan kan bli belastet slik at det blir mindre brukbart for den rettmessige innehaveren (tilgjenglighet). Datainnbruddet er handlingen som gir gjerningspersonen tilgang til å foreta slike ytterligere handlinger på datasystemet. Et datainnbrudd har derfor ofte karakter av en handling som på en eller annen måte bryter sperrer som er satt til å verne om systemet." (NOU 2007: 19, side 22) Former for datainnbrudd inkluderer bruk av[27]

- ondsinnet programvare,

[26] http://www.facebook.com/terms.php?ref=pf

[27] En ikke-uttømmende liste.

- sårbarhetsinnbrudd og
- passordknekking

4.3.3 Risikovurdering

Både Facebook og CDON driver innsamling og behandling på et lovlig grunnlag gjennom samtykke fra hver enkelt bruker, jf. personopplysningsloven § 8 første ledd. De kritiske punktene ved løsningene synes å knytte seg til

- sikring av kommunikasjonsdata mellom bruker og tjenestetilbyder,
- sikring av personopplysninger sentralt,
- sikring av autentiseringsinformasjon hos bruker og
- sikkerhet for at riktig bruker blir autentisert.

De tre første punktene omhandler *konfidensialiteten* og *integriteten* til elektronisk lagrede personopplysninger, og er truet i en første fase av et identitetstyveri. Trusler knyttet til autentisering av brukere omhandler sikkerhet for at brukeren som identifiserer seg er den han utgir seg for å være og kan knyttes til den siste fasen av et identitetstyveri som jeg skal komme tilbake til i avsnitt 4.4.

4.3.3.1 Datainnbrudd

Datainnbrudd skjer ved å omgå fysiske sperrer i et system for å skaffe seg uberettiget tilgang til et datasystem. En måte å gjøre dette på er å identifisere *sårbarheter*. En sårbarhet er et sikkerhetshull som gjør det mulig for personer med tilstrekkelig kunnskap, eller med riktig teknologi å få tilgang til andres maskiner ved å bruke *ondsinnet programvare*. Ondsinnet programvare som brukes til å utnytte sårbarheter kalles for *exploits*, og kommer i form av eksempelvis *trojanere* og *keyloggers*[28]. En trojaner er programvare som skjuler seg i det som i utgangspunktet ser ut som et helt harmløst program. Når dette programmet utføres slippes koden løs og angriper en brukers maskin ved å ta kontrollen over den eller ved å overvåke brukeren på andre måter. En vanlig måte for en trojansk hest å fungere på er ved å åpne porter slik at maskinene den opererer på blir åpen for andre typer angrep (Linninger & Vines 2005, side 117). Keyloggers er små program som logger tastetrykk i en tekstfil som deretter sendes til angriperen. Alt brukeren skriver på tastaturet, inkludert sensitiv påloggingsinformasjon vil på denne måten komme på avveie uten av brukeren er klar over det selv.

[28] Det finnes også mange flere uten at jeg ser det som relevant å foreta en ufyllende presentasjon. For mer om slike se Linninger & Vines 2005.

Sårbarheter finnes i alle typer software: nettlesere, operativsystem og alle andre små eller store tileggsprogram en bruker kan installere på sin maskin. I følge NorSIS er alt som trengs for å utnytte sårbarheter at man er i besittelse av IP-adressen til den maskinen man ønsker å bryte seg inn på[29]. IP-adresser benyttes i all kommunikasjon mellom brukerens maskin og de tjenestene eller nettsidene brukeren besøker. Ved hjelp av relativt enkle metoder er dermed IP-adresser tilgjengelige for den som måtte ønske[30]. Sårbarhetsinnbrudd kan ramme både individuelle brukere og behandlingsansvarlige.

CDON har enveiskryptering av sensitiv informasjon. Når en bruker skriver inn kredittkortinformasjon krypteres informasjonen når brukeren bekrefter og sender disse opplysningene. Krypteringen som brukes er SSL (Secure Socket Layer) sertifikat med Camellia-256 som er en 256 bit høygradskryptering. SSL er en kryptografisk protokoll for sikker kommunikasjon på internett[31]. Dette er regnet som en svært sikker løsning, og benyttes blant annet av EUs NESSIE-prosjekt (New European Schemes for Signatures, Integrity and Encryption). Ved innlogging benytter CDON RC4 128 bits kryptering som av Sun Microsystems, en av verdens ledende programvareselskaper, regnes som den nest sterkeste krypteringen som finnes i dag. CDON selger for øvrig både fysiske produkter og nedlastbar musikk. Ved kjøp av nedlastbare musikkfiler blir brukeren for øvrig bedt om å logge inn på nytt. Tilsvarende innlogging er imidlertid ikke kryptert. Facebook benytter også SSL når brukeren sender sensitiv informasjon. I likhet med CDON er det RC4 kryptering som benyttes. Facebook oppgir også at databasen deres befinner seg på en sikker server beskyttet med brannmur. CDON nøyer seg med å oppgi at de tar i bruk både organisatoriske og tekniske virkemidler for å beskytte integriteten i de lagrede dataene.

Det er foreløpig få kjente eksempler på hendelser i Norge hvor behandlingsansvarlige har blitt utsatt for datainnbrudd og personopplysninger har kommet på avveie. I følge mørketallsundersøkelsen for

---

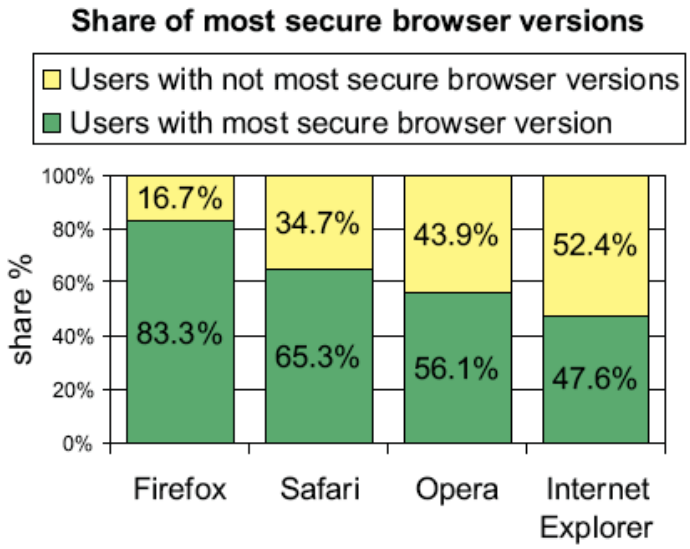
29 http://www.dagbladet.no/2009/04/21/magasinet/datasikkerhet/hackere/hacking/informasjonsteknologi/5582119/

30 http://www.nettsikkerhet.info/html/150706_news001_ipadresse.html
Se også NOU 2007: 19 avsnitt 3.4.2 som tar for seg elektronisk kartlegging av sårbarheter og identifisering nettadresser.

31 http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/

2008 var det imidlertid estimert 4400 tilfeller av datainnbrudd blant ulike behandlingsansvarlige mens bare 57 hendelser ble anmeldt. (Ellertsen 2008) Det er derfor rimelig å anta at behandlingsansvarlige på nett er mer utsatt enn det man får inntrykk av gjennom rapporterte hendelser. Det mest kjente tilfellet var likevel da en rekke teleselskaper i 2007 ble offer for et automatisert program som hentet ut personnummer og adresser tilhørende mange tusen nordmenn[32]. Det finnes også eksempler på alvorlige sikkerhetshull med BankID som er bankenes mekanisme for sikker autentisering av brukere. For noen år tilbake ble det oppdaget en metode som gjorde det mulig å få nettbanken til Skandiabanken til å godta falske sertifikater, og flere ganger i 2007 klarte en professor sammen med noen studenter å komme seg enkelt forbi sikkerhetsmekanismene i en senere og mer avansert versjon av BankID.

Internasjonale undersøkelser viser at brukere er særlig utsatt for datainnbrudd. En undersøkelse foretatt av forskere fra Google, IBM og Computer Engineering and Networks Laboratory i Zürich foretatt i perioden januar 2007 til juni 2008 viste at 45,2 prosent av nettleserbrukere verden over ikke hadde oppdatert til nyeste versjon av nettleseren sin. Dermed var disse ekstra utsatt for utnyttelse av kjente sårbarheter. (Frei et al 2008, side 4)



Figur 31: Andel av brukere med ulik nettleser som benyttet seg av den nyeste utgaven av sin nettleser i Juni 2008 (Frei et al. 2008, side 4)

Alle nettlesere har én eller flere såkalte plug-ins. En plug-in er et programvaretillegg som blir installert i nettlesere for at denne skal kunne vise forskjellige typer web-elementer. Det er opp til

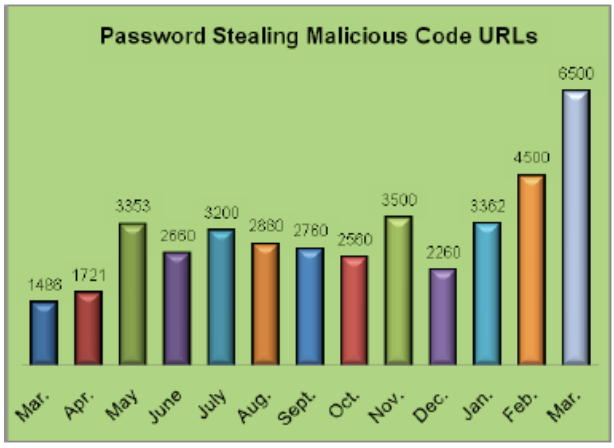
[32] http://www.digi.no/392221/tyver-stjal-60000-personnummer

hver enkelt bruker å innstaller slike selv, men hver gang det dukker opp innhold nettleseren ikke kan vise vil brukeren få spørsmål om hvorvidt han ønsker å installere et programvaretillegg. Blant disse finner vi Flash Player som gjør det mulig å vise avanserte animasjoner eller Windows Media Player som brukes for å video i en nettside. For at en nettleseren skal kunne gjøre de tingene man forventer til daglig må man altså basere seg på å installere ett eller flere slike. Jeg har ikke funnet tallmateriale som kan fortelle noe om hvor mange brukere som benytter seg av utdatert programtillegg, men det er ingen grunn til å anta at folk flest er flinkere til å oppdatere slike enn annen type software. Det er heller grunn til å tro det motsatte. Dette fordi det i stor grad er opp til brukeren selv å oppdatere programvaren mens man med et operativsystem kan sette systemet til å automatisk sjekke etter slike. Figur 8 viser utbredelsen av populære programvaretillegg, og dermed også at det potensielt er mange brukere som ikke har oppdaterte versjoner av disse.

Plug-In	Vendor	Share	Support
Flash Player	Adobe	98.8%	all
Java	Sun	84.0%	all
Media Player	Microsoft	82.2%	IE only
QuickTime Player	Apple	66.8%	all
Shockwave Player	Adobe	55.6%	all
RealOne Player	Real Networks	47.1%	all
Acrobat PDF Reader	Adobe	>80%	all

Figur 32: Utbredelsen av populære Plug-Ins (Frei et al 2008, side 5)

Datainnbrudd på en brukers maskin er av interesse fordi mange brukere benytter seg av ulike løsninger for å oppbevare elektroniske identiteter og andre personopplysninger lokalt på maskinen sin. Blant annet kan man få nettleseren til å huske elektroniske identiteter og på den måten både unngå å måtte huske brukernavn og passord samtidig som nettleseren besørger at denne informasjonen er ferdig utfylt for brukerne i påloggingsfeltene. Ved tilfeller av datainnbrudd vil denne informasjonen være tilgjengelig for uvedkommende. Ved pålogging i nettbanker vil dette ikke være mulig fordi de tekniske løsningene ikke tillater brukere å gjøre dette. Både Facebook og CDON gir imidlertid brukerne mulighet for å lagre sin elektroniske identitet i nettleseren og øker dermed skadepotensialet for brukeren ved et eventuelt datainnbrudd.



Figur 33: Bruken av ulike typer ondsinnet programvare stiger dramatisk i følge Anti Phishing Working Group (APWG 2008, side 2)

Passordknekking foregår ved å bruke automatiserte program som tester et stort antall mulige tegnkombinasjoner mot en påloggingsløsning helt til den finner en kombinasjon som blir akseptert. Desto færre tegn et passord består av, dess færre kombinasjoner er det for et passordknekkingsprogram å teste. Samtidig som et passord bør bestå av mange og forskjellige typer tegn for å være sikkert mot passordknekking er det også farer knyttet til dette. Brukere som blir pålagt å opprette lange kompliserte passord for mange ulike tjenester kan fort velge å bruke det samme passordet for mange ulike tjenester. Noen vil kanskje også gå til det skritt å skrive det ned. Lange kompliserte passord *kan* derfor også medføre motsatt effekt av det man ønsker.

I følge Norsk Senter for Informasjonssikkerhet (NorSIS) bør et passord ha minimum 8 tegn og bestå av kombinasjoner av flere typer tegn[33]. Passord med færre tegn er spesielt utsatt for relativt enkle program. Enkle tekniske forhåndsregler er imidlertid det som skal til for å hindre slike program, som ved å legge begrensning på hvor mange ganger en bruker kan taste feil passord før kontoen for eksempel blir midlertidig utilgjengelig.

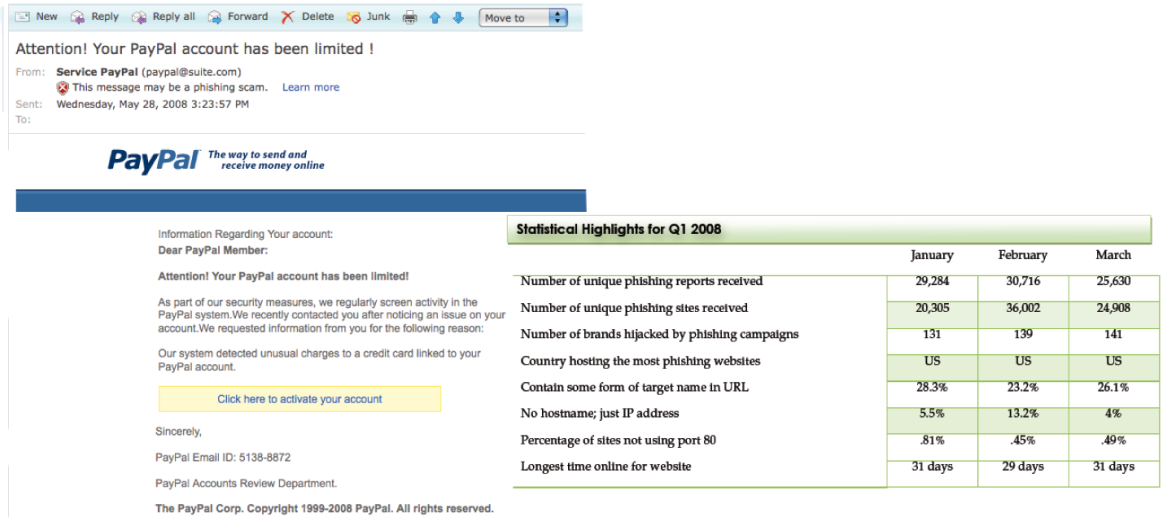
Ingen av tjenestene synes imidlertid å ha lagt inn sperre på hvor mange ganger en bruker kan taste feil passord. Samtidig kreves det ikke av brukeren at passordet må være av en viss lengde eller skal bestå av kombinasjoner av tegn og tall. Dette gjør det mulig å bruke automatiserte program for å knekke passordløsningen dersom man har et brukernavn. Brukernavnet er i begge tilfeller brukerens e-post, noe som imidlertid gjør det mulig å kjøre lister med innsamlede e-postadresser mot systemet sammen med et program for å knekke passord.

[33] http://www.norsis.no/veiledninger/Passord.html

4.3.3.2 Sosial manipulering

Phishing er en teknikk for å manipulere brukere til å frivillig avgi personopplysninger ved å utgi seg for å være noen man ikke er. Henvendelse av denne typen kommer i form av falske mail eller falske nettsider, og er hybride teknikker som kombinerer teknologi med sosial manipulering gjennom å bruke digitale medier som arena og overbevisningens kraft som metode. Særlig er en phisher ute etter påloggingsinformasjon som danner grunnlag for identitetsforedling og identitetssvindel.

Senest i mai 2009 kom det meldinger om at Facebook hadde blitt utsatt for et phishing angrep[34], noe som demonstrerer at *brukere* av slike tjenester er utsatt for slike typer av angrep. At slike typer angrep representerer en stor trussel for den enkelte bruker bekreftes også av internasjonal statistikk. Anti Phishing Working Group (APWG) kunne vise til at nærmere hundretusen unike phishing nettsider ble rapportert inn i løpet av første kvartal i 2008.



Figur 34: Eksempel på phishing-mail samt Statistikk fra første kvartal 2008 (APWG 2008, side 3)

Det er vanskelig å danne seg et fullstendig bilde av risikoen forbundet med de ulike truslene fordi det er lite materiale tilgjengelig som gjør det mulig å konkludere. Det synes imidlertid klart at brukerne selv i stor grad har et ansvar for å sikre egen elektroniske ressurser og at det ligger et betydelig forbedringspotensialet her. Brukerne fremstår i så måte som et langt enklere mål fremfor tjenesteleverandører som i større grad virker å være beskyttet. På tross av et uklart bilde mener jeg

[34] http://www.itavisen.no/813455/massivt-angrep-mot-facebook
http://www.norsis.no/nyheter/2009-05-13-Facebook-spam.html

likevel at fremstillingen gir gode argumenter for at alle overnevnte trusler representerer en reell overhengende fare i forbindelse med identitetstyveri.

Det er imidlertid ikke bare teknologiske teknikker som truer konfidensialiteten og integriteten til personopplysninger. På tross av stort fokus på nettopp slike teknikker skal vi se at det også finnes betydelige farer forbundet med personopplysninger i et fysisk format.

4.4 Nærmere om ikke-tekniske trusler

4.4.1 Identifiserte trusler

Tilegnelse av personopplysninger kan skje på andre måter enn gjennom rent tekniske metoder. Personinformasjon tilegnet gjennom bruk av slike metoder kan senere benyttes til å gjennomføre identitetssvindel i nettbaserte kanaler.

- Tyveri
  - post
  - søppel
  - identitetsbevis
- Uthenting av informasjon fra gammel PC-utstyr
- Søking i offentlige registre
- Skimming
- Utro tjenere,

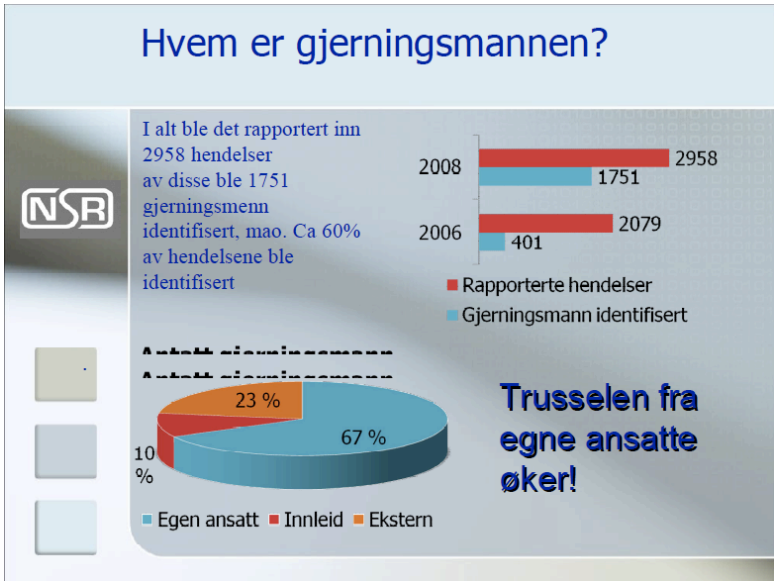
Selv om mye kommunikasjon foregår elektronisk, kommer mye informasjon fremdeles i fysisk form: selvangivelsen, bank- og kredittkort, pinkoder og lignende. Tyveri av post og søppel er derfor en potensielt trussel som kan muliggjøre identitetstyveri. Samtidig er det et kjent og vanlig fenomen å både miste og å bli frastjålet bankkort. Også i gammel datautstyr kan det finnes mye informasjon som kan hentes frem av kyndige personer selv om eieren tror maskinen er ubrukelig og ødelagt. Lagrede e-post, brukernavn og passord er ikke uvanlig at lagres, og slike kan inneholde mye informasjon som potensielt kan bruks som ledd i et identitetstyveri.

Mye informasjon kan også være tilgjengelig i offentlige registre, blant annet i skattelistene som hvert år legges ut på nett hos skatteetaten og samtlige store nettaviser i landet. Offentlige registre inneholder neppe nok informasjon til å i seg selv muliggjøre identitetstyveri, men Datatilsynet har

påpekt at ukritisk publisering av personopplysninger i eksempelvis offentlige journaler eller registre er en trussel mot den enkeltes personvern i forhold til identitetstyveri. (Datatilsynet 2009, side 15)

Skimming er en teknikk for å kopiere magnetstripen på et kredittkort, eller et hvilken som helst annet kort med magnetstripe. Ved hjelp av en skimmer, som er en liten kortleser, kan man enkelt overføre all informasjonen som ligger i magnetstripen over på en data. Om man i tillegg har en kodingsenhet for kredittkort kan man duplisere kortet så mange ganger man måtte ønske[35]. Det finnes mange måter å bruke slike skimmere på. En velkjent metode som har fått mye oppmerksomhet i Norge de siste årene er skimmingutstyr montert på minibanker, gjerne kombinert med et lite kamera som fanger opp pinkoden brukeren taster inn. En annen metode er at medarbeidere i eksempelvis servicenæringen med tilgang til kunders kredittkort også kan kopiere magnetstripene ved hjelp av en skimmer.

Sikkerheten i en hvilken som helst bedrift vil aldri være bedre enn det svakeste ledd. I mange tilfeller er dette leddet en utro medarbeider som utleverer informasjon til utenforstående for et gitt pengebeløp. I følge mørketallsundersøkelsen for 2008 gjennomført av Næringslivets Sikkerhetsråd viste at nærmere 70 prosent av uønskede hendelser knyttet til datakriminalitet i norske bedrifter ble utført av egne ansatte[36].



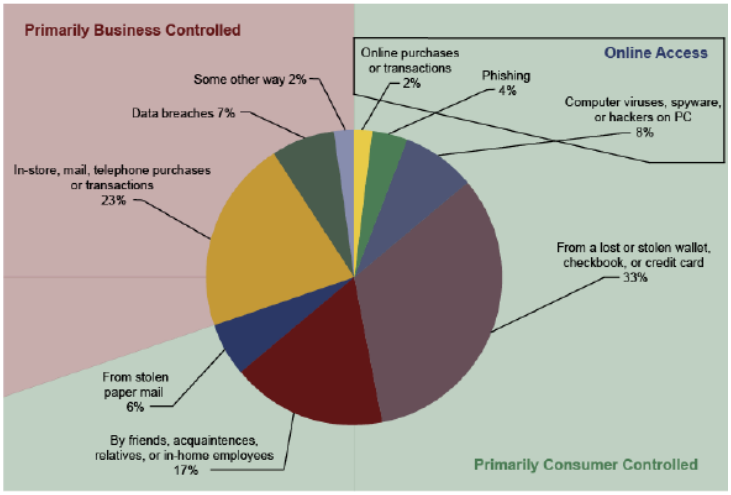
Figur 35: Utro tjenere i norske bedrifter (Ellertsen 2008)

[35] http://en.wikipedia.org/wiki/Image:Credit_Card_Fraud_Skimming_Video.ogg

[36] Tallene er knyttet til datakriminalitet generelt og ikke personopplysninger spesifikt.

4.4.2 Risikovurdering

Risikoen for fysisk tyveri av informasjon er for mange overhengende. I følge Datatilsynet finnes det for eksempel svært mange ulåste postkasser i Norge[37], noe som gjør det svært enkelt å komme i kontakt med sensitive personopplysninger om andre. Figur 16 er basert på en undersøkelse utført av Javelin Research i USA i 2007, og viser at majoriteten av personopplysninger på avveie ble tatt fra nettopp brukerne selv. Uberettiget tilegnelse av personinformasjon på internett utgjør foreløpig bare en liten del av totalen: 14 prosent for brukere og 7 prosent gjennom sikkerhetsbrudd hos behandlingsansvarlige.



Figur 36: Statistikk for uberettiget tilegnelse av personopplysninger 2007 (Javelin Research 2008)

Hvorfor identitetstyveri likevel ofte blir omtalt i sammenheng med elektroniske løsninger kan være fordi potensialet i dette er enormt. Èn kundedatabase kan inneholde alt fra noen hundre til noen millioner kunder, og når alt er tilgjengelig over internett kan bare ett datainnbrudd medføre konsekvenser for mange mennesker. Likevel viser tallene i tabellen over at det fremdeles er mer utbredt med tyveri av informasjon gjennom tyveri eller uærlig venner, ansatte og familie. Det kan være flere grunner til å se på tallene i figur 16 med noe skepsis. Mange kan ha blitt fratatt informasjon gjennom tekniske metoder uten selv å vite at noe har skjedd, eller blitt overbevist om å oppgi informasjon on-line på falske premisser uten at man er klar over den egentlige hensikten bak. Dersom denne informasjonen blir misbrukt lang tid i etterkant er det vanskelig å vite hvor og

[37] http://arkiv.nettavisen.no/Nyhet/218650/-+L%C3%A5s+postkassa.html
http://www.digi.no/370321/datatilsynet-vil-ha-laaste-postkasser

hvordan informasjonen eventuelt har kommet på avveie. Fysisk tyveri er derimot enklere å oppdage fordi noe fysisk er borte.

4.5 Trusler knyttet til autentisering

Hensikten med autentiseringsmekanismer er å bekrefte en påstått identitet og har primært som formål å hindre at en bruker kan utgi seg for å være en annen bruker. Dermed er vi inne på kjernen i et identitetstyveri. Autentiseringsmekanismer kan være sterke eller de kan være svake, noe som avhenger av hva man velger som *autentifikator*. Truslene knyttet til autentisering av brukere handler derfor i stor grad om valg av autentifikator som gir tilstrekkelig sikkerhet mot at andre kan autentiseres med en annens identitet. En slik vurdering avhenger av hvor stor grad av sikkerhet mekanismen må kunne fastslå en identitet med. Gir tjenesten tilgang til personopplysninger, og gjerne sensitive personopplysninger kreves det større grad av sikkerhet og dermed sterkere mekanismer. Er det derimot nok vite at brukeren er innehaver av en rolle som kunde eller ansatt eller er innehaver av en spesiell attributt vil det ikke være nødvendig eller ønskelig å benytte seg av sterke mekanismer som krever bruk av personopplysninger. Autentisering kan i følge Thomas Olsen dermed foregå på flere nivå: (NOU 2009:1, side 287)

- Individ
- Rolle
- Attributt

På alle nivåer vil imidlertid farene knyttet til identitetstyveri være knyttet til hvor enkelt det er bli autentisert som en annen enn den man er mens konsekvensene avhenger av hva autentiseringen gir tilgang til av informasjon. Hos Facebook og CDON er det e-post som er identifikator mens et selvvalgt passord er autentifikator, jf. 4.3.3.1. Det er med andre ord en svak én-faktor autentisering med utgangspunkt i noe brukeren *vet* eller *har*. Facebook er som vi har sett en tjeneste som kan brukes uten å oppgi personopplysninger samtidig som det også vil kunne befinne seg mye personopplysninger i en brukerkonto. CDON krever fødselsnummer og i visse tilfeller også personnummer.

Trusler knyttet til autentisering gjør seg også gjeldende i den fysiske verden og kan illustreres blant annet i forbindelse med adresseendring hos posten og folkeregisteret. Jeg kommer tilbake til dette i neste avsnitt i forbindelse med metoder knyttet til identitetsforedling.

4.6 Nærmere om metoder knyttet til identitetsforedling

4.6.1 Adresseforandring og utnytting av folkeregistrert adresse

Adresseforandring hos posten og hos folkeregisteret sikrer full tilgang til og kontroll over informasjonsflyten i en persons hverdag, og er derfor spesielt interessant å se litt nærmere på. Dermed muliggjør man identitetsforedling ved å bestille informasjon, gjerne sensitiv informasjon, som blir tilsendt folkeregistrert adresse uten videre autentisering av bruker. Mekanismene for å kunne melde adresseforandring har de seneste par årene blitt forbedret. Ønsker man å gjøre det via nett må man autentisere seg via MinID, som jeg kommer tilbake til i kapittel 5. Kort fortalt er MinID en elektronisk identitet som autentiserer brukere ved hjelp av både pinkoder, passord og fødselsnummer. Alternativt må man møte opp med legitimasjon på posten eller sende flyttemelding med kopi av identitetsbevis til folkeregisteret. Godkjent identitetsbevis skal inneholde fødselsdata, navn, signatur og bilde og kan være et studentkort for eksempel. Unntaket her er bankkort, som grunnet sensitiv informasjon på baksiden ikke kan brukes. Har man tilgang på et slikt kan man forandre den folkeregisterte adressen til hvem det måtte være. Adresseforandringen trer i kraft så snart det fattes vedtak, og det blir deretter sendt melding om vedtaket til adressen som er blitt endret. Dermed har man et ”vindu” på noen få dager fra enkeltvedtaket om flytting blir iverksatt og frem til melding om vedtaket når frem til adressen som skal endres.

Det er imidlertid ikke sikkert det er nødvendig å gå til det skritt å endre adressen. Svært mange husstander i Norge har ingen sikring på postkassene sine slik at disse står åpne for at uvedkommende kan stjele post, jf avsnitt 4.4.1. Dermed kan det være tilstrekkelig å bestille informasjon til folkeregistrert adresse for deretter å stjele forsendingen fra en åpen postkasse. I de fleste tilfeller er fødselsnummer, kanskje kombinert med navn, alt som trengs for å bestille sensitiv informasjon om en person fra det offentlige. Dette gjelder eksempelvis i forhold til bestilling av pinkoder til MinID, som gir tilgang til det meste av informasjon det offentlige har registrert på hver enkelt av oss. Dermed synes det som om folkeregistrert adresse er ansett som en sikkerhetsmekanisme i seg selv.

4.6.2 Utnytting av elektroniske identiteter

Gjennom å sikre seg tilgang til elektroniske identiteter, jf definisjonen i avsnitt 1.4.4, kan man bruke disse til å be om innsyn i registrerte opplysninger og slik bygge opp en personprofil. Ved å få tilgang til en e-postkonto vil man for eksempel kunne tilegne seg både brukernavn og passord til en rekke tjenester den aktuelle brukeren er innehaver av. Dette får man fordi de aller fleste

registreringstjenester på internett sender brukernavn og passord til en e-post brukeren selv oppgir[38]. Dersom brukeren ved senere anledninger glemmer passordet vil man også kunne få dette tilsendt på nytt til den samme e-posten. Tjenester som Facebook og CDON vil kunne være spesielt interessante i en videreforedlingsfase da ingen av tjenestene behandler opplysninger av sensitiv art[39]. Begge disse gjør det mulig å kartlegge kjøpsvaner, interesser, reisevaner, fremtidsplaner og mye mer som kan gå inn i en personprofil.

Tilegnede personopplysninger kan videre brukes til å begå identitetssvindel.

4.7 Konsekvenser av identitetstyveri

Konsekvensene av et identitetstyveri finnes på to nivå:

- individnivå
- samfunnsnivå

Det foreligger ingen statistikk i Norge på omfanget av identitetstyveri og ei heller konsekvensene det får for den enkelte som blir rammet. I USA finnes det derimot tilgjengelig tallmateriale fra flere år tilbake.

[38] Dette gjelder blant annet Facebook og CDON

[39] CDON behandler fødselsnummer, som selv om det ikke er sensitivt heller ikke skal utleveres til hvem som helst.

		Survey Report				
	Trend	2008	2007[1]	2006	2005	2003
US adult victims of identity fraud[2]	↓	8.1 M	8.4 M	8.9 M	9.3 M	10.1 M
Fraud victims as % of US population	↓	3.58%	3.84%	4.00%	4.25%	4.70%
Total one year fraud amount[3]	↓	$45 B	$51 B	$58 B	$57 B	$56 B
Mean fraud amount per fraud victim	↓	$5,574	$6,920	$6,497	$6,203	$5,503
Median fraud amount per fraud victim	■	$750	$750	$750	$750	$750
Mean consumer cost	↑	$691	$554	$446	$711	$582
Median consumer cost	■	$0	$0	$0	$0	$0
Mean resolution time (hours)	↑	26 hrs.	25 hrs.	40 hrs.	28 hrs.	33 hrs.
Median resolution time (hours)	■	5 hrs.	5 hrs.	5 hrs.	5 hrs.	5 hrs.

Figur 37: Amerikansk statistikk 2003-2008 (Javelin Research 2008, side 1)[40]

Tallene viser at identitetssvindel i USA har flatet ut og gått noe ned de siste 3 årene. Fremdeles ble likevel over 8 millioner amerikanere rammet i 2008, noe som resulterte i gjennomsnittlig 26 timers arbeid og nærmere $ 700 i kostnader for den enkelte.

Konsekvensene for den enkelte som rammes vil være avhengig av i) hvor mye personopplysninger som er på avveie og ii) hva slags type opplysninger dette gjelder. De enkleste formene som ifølge CIPPIC og identitetstyveriprosjektet kan karakteriseres som identitetstyveri vil gå rett fra tilegnelse av personopplysninger i første fase til identitetssvindel i tredje fase uten noen form for identitetsforedling. Kopiering eller tyveri av bankkort for deretter å bestille varer over nett er klassiske eksempler på dette. Slike tilfeller vil ha begrensende konsekvenser fordi den som rammes med relativt enkle midler vil kunne rette opp skaden ved at bankkortet sperres. Banken vil dermed sitte igjen med tapet ved senere off-line (VISA) aktivitet på kortet[41]. Utover opplysinger knyttet til kortnummer og CVC kode som muliggjør handel over nett er det ikke andre opplysninger i tilknytning til kortet som alene vil kunne påføre stor skade. I tilknytning til andre opplysninger vil imidlertid dette kunne danne grunnlaget for systematisk og gjentatt identitetssvindel, noe som vil kunne ramme den enkelte hardt over lang tid.

Av de tre aktørene som i kapittel 2 ble identifisert som involvert i et identitetstyveri synes det som om identitetsholderen i form av en enkeltperson er den som blir rammet hardest. Konsekvensene for

[40] M= million, B=billion

[41] Med mindre kunden har opptrådt uaktsomt.

individet kan for det første være av økonomisk karakter gjennom kredittkortmisbruk eller opptagelse av lån i en annens navn, men kan også være av ikke-økonomisk karakter gjennom den psykiske belastningen det kan være å vite at noen andre bruker ens identitet. Utstrakt og gjentatt misbruk medfører at identitetsholderen må bruke mye tid og ressurser på å ordne opp, fordi det per i dag ikke finnes noe sentralt sted å henvende seg for å få hjelp. Det finnes heller ikke noen felles tjeneste for å melde fra om misbruk av egen identitet. Identitetsholderen er dermed selv avhengig av å kontakte relevante aktører, for eksempel kredittopplysningsbyrå for å sperre personnummeret for kredittsjekk slik at kredittmisbruk og banken for å sperre kredittkortet slik at fremtidig bruk ikke blir belastet offeret. Konsekvensene av dette er igjen at det i tilfeller hvor identitetsholder har et behov for å få gjennomført en kredittvurdering vil dette bli en tungvint affære fordi man da må oppheve sperren for så å innføre den på nytt etter gjennomført vurdering. Identitetsholderen kan i tillegg måtte sperre tilgangen til adresseendring både hos folkeregisteret og posten for å hindre uønsket adresseendring. Identitetstyveri av ikke-økonomisk karakter kan videre få konsekvenser i form av tapt anseelse fordi identitetsholderen blir tillagt meninger og holdninger han ikke har. I verste fall kan man tenke seg en situasjon hvor identitetsholderen mister muligheten til å få en jobb han har søkt på eller mister en jobb han allerede har. Konsekvensene for den enkelte øker i takt med omfanget av identitetssvindelen, og blir dermed spesielt omfattende i saker med målrettet identitetstyveri og bruk av identitetsforedling.

På samfunnsnivå kan tilliten til systemet, og tilliten til elektronisk kommunikasjon spesielt bli utfordret. Som oftest må man kunne anta at finansinstitusjonene til slutt sitter igjen med regningen når det er stadfestet at et økonomisk relatert identitetstyveri har forekommet. Mens den enkelte av oss stort sett har begrensede ressurser og begrenset kapasitet til å følge opp og ordne opp vil imidlertid bedrifter og andre institusjoner ha et helt annet utgangspunkt. Juridisk kompetanse, forbindelser til media samt finansielle muskler er argumenter som demonstrerer den store forskjellen fra mannen i gata som alene må stå opp imot systemet.

4.8 Konklusjon og overgang til kapittel 5

Identitetstyveri kan potensielt gå gjennom tre faser: tilegnelse, videreforedling og misbruk av bruker- og personopplysninger. Videreforedlingsfasen synes å være elementet som gir et identitetstyveri dimensjonen av mangel på kontroll for den som blir rammet. Gjennomgangen i dette kapittelet har avdekket at identitetstyveri er mulig av to grunner:

- svak sikring av *konfidensialiteten* og *integriteten* til lagrede eller fysiske personopplysninger

- svak *autentisering* som autoriserer brukere til ressurser eller tjenester

Svak sikring av konfidensialitet muliggjør uberettiget tilegnelse av person- og brukeropplysninger og mottiltak handler om å sikre *integriteten* til lagrede person- og/eller brukeropplysninger. Sikring av konfidensialitet er et ansvar som må bæres av både behandlingsansvarlige og brukere fordi person- og brukeropplysninger ikke bare lagres sentralt hos behandlingsansvarlige men finnes også lokalt hos bruker. Brukerne selv har dermed et betydelig ansvar for å sikre egne elektroniske og fysiske ressurser mot uautorisert tilgang. Gjennomgangen har imidlertid vist at angrep mot individuelle brukere er det som truer konfidensialiteten til lagrede data mest. En av grunnene til dette kan være at mange brukere utsetter seg for fare gjennom utdatert programvare som blottlegger dem for ulike typer datainnbrudd, mens behandlingsansvarlige i større grad har adekvat sikkerhet som krever større innsats for å trenge gjennom. Autentisering av brukere handler om grad av sikkerhet for at den identifiserte brukeren er den han utgir seg for å være. Ansvaret for disse mekanismene ligger utelukkende hos tjenestene. Tabell 2 under viser trusler, uønskede hendelser knyttet til truslene, hvor stor sannsynlighet jeg vurderer hendelsene til å ha og konsekvensen av hendelsene.

Faser	***Trusler***	***Uønskede hendelser***	***Sannsynlighet***	***Konsekvens***
Tilegnelse	Konfidensialitets og integritetsbrudd	Datainnbrudd, sosial manipulering, ulike typer tyveri, utro tjenere, skimming, søking i offentlige registre.	Stor: mye personopplysninger havner på avveie.	Moderat: langt fra alle opplysningene blir noen gang brukt.
Videreforedling	Konfidensialitet, integritet og autentisering	Adresseforandring, utnytting av elektroniske identiteter	Liten: foredling skjer i relativt liten grad.	Stor: medfører systematisk og gjentatt identitetstyveri.
Svindel	Svak autentisering	En bruker blir akseptert med en annen identitet enn dens egen.	Stor: mange svake autentiseringsmekanismer gjør dette forholdsvis enkelt.	Stor: medfører økonomisk tap og/eller krenkelse.

Tabell 2: Oversikt risikoanalyse

Truslene jeg har identifisert i dette kapittelet skal jeg ta med videre inn i kapittel 5 hvor jeg skal se på tiltak som kan være med å redusere risikoen for identitetstyveri. Kapittelet kommer til å ha spesielt fokus på tekniske løsninger som tiltak mot elektronisk identitetstyveri.

Kapittel 5: Tiltak for å bekjempe identitetstyveri

5.1 Innledning

I kapittel 4 beskrev jeg prosessen i et identitetstyveri og identifiserte trusler mot både elektronisk og fysisk lagrede personopplysninger. I dette kapittelet skal jeg se på alternativer for hvordan truslene kan motvirkes gjennom ulike tekniske og organisatoriske tiltak. Dette kapitelet er dermed siste delen av sikkerhetsarbeidet påstartet i kapittel 4. Tiltakene jeg skal se på er *forebyggende*.

Innledningsvis skal jeg se på hvordan og i hvilke situasjoner personvernøkende teknologi kan spille en rolle. Jeg skal deretter rette fokuset mot modeller for identitetsforvaltning, og kommer til å fokusere på føderert identitetsforvaltning som muliggjør utveksling av identitetsdata på tvers av organisasjonsplattformer. I den forbindelse skal jeg se nærmere på standarden for føderert identitetsforvaltning SAML 2.0 og eksemplifisere gjennom hvordan denne er implementert i MinID og FEIDE. Hovedfokuset er imidlertid på standardens overordnede prinsipper og ikke minst potensial fremfor å være detaljerte og grundig i gjennomgangen. Jeg skal videre se på bruk av biometri som alternativ for sikker identifisering og autentisering før jeg avslutningsvis adresserer tiltak mot ikke-tekniske trusler. Det er ikke kapitelets hensikt å komme med bastante konklusjoner, men heller å identifisere alternative løsninger og diskutere dem mot hverandre.

5.2 Personvernøkende teknologi og anonymitet som tiltak mot identitetstyveri

Personvernøkende teknologi (PETs) har tradisjonelt vært knyttet til å gi den enkelte bruker større kontroll over egen identitet gjennom anonymisering eller pseudonymisering av identitet. Det avgjørende for om et identitetstyveri kan forekomme er tilstedeværelsen av personopplysninger. Dermed aktualiseres spørsmålet om anonymitet eller pseudonymitet kan bidra til å redusere farene for identitetstyveri.

5.2.1 Anonymitet

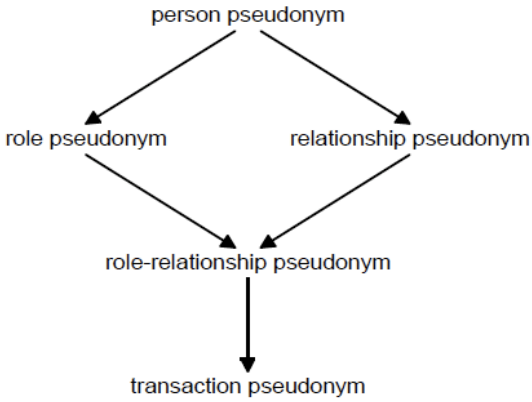
Retten til å være anonym er et omstridt spørsmål fordi det neppe er i samfunnets interesse at elektroniske medier blir en frisone for kriminelle. Anonymitet kan imidlertid også være med på å bygge opp under essensielle elementer i et fungerende demokrati, blant annet retten til å avgi stemme anonymt og retten til å ha kontroll over egen identitet. I Storingsmelding nr. 17 2006-2007 *Eit informasjonssamfunn for alle* ble det påpekt at mulighetene til fortsatt anonym kommunikasjon

på nett er viktig. Stortingsmeldingen fremhevet derfor en rekke viktige tiltak og satsninger for å sikre ivaretakelsen av personvernet på en best mulig måte, blant annet viktigheten av å sørge for mulighetene for anonym eller pseudonym kommunikasjon. Dette var en følge av regjeringens erkjennelse av at nettopp økt bruk av *sikker* personidentifisering er et av utviklingstrekkene i dagens samfunn, uten at identifiseringen strengt tatt er nødvendig. (St.mld. nr.27, side 131)

Muligheten til å være anonym er viktig av flere grunner slik jeg ser det. Det er blant annet et vesentlig poeng at den enkelte har rett på en privat sfære også i det offentlige rom. Med identifisering av individ følger behandling av personopplysninger, og med det følger også faren for identitetstyveri. Samtidig er det også et viktig personvernprinsipp å kunne ferdes og opptre anonymt i den grad det ikke er et saklig behov for identifisering. Mange elektroniske identitetsforvaltningsløsninger i dag legger opp til utstrakt innsamling av personinformasjon for bruk av tjenester som man fra den fysiske verden kunne gjort anonymt eller i hvert fall uten at transaksjonen logges, lagres og kan knyttes til individet ved en senere anledning. I forbindelse med høringsnotatet som første gang foreslo strategi for eID og eSignatur i offentlig sektor, uttrykte Datatilsynet bekymring for overeksponering av identitetsdata i interaksjon med det offentlige. Dette fordi man mente det ville oppstå usikkerhet rundt hvor sterk identifisering ulike tjenester skulle kreve. Utstedelse av offentlig eID ville dermed etter Datatilsynets skjønn stå i fare for å kreve både for mye og for sterk identifisering og autentisering der hvor det ikke var behov for dette. (Datatilsynet 2007, side 1) Dette må samtidig balanseres mot det behovet samfunnet i mange tilfeller har for å vite hvem man kommuniserer med, spesielt dersom det offentlige for eksempel skal kunne tilby personlige elektroniske tjenester.

5.2.2 Pseudonymitet

Anonymitet markerer et ytterpunkt på en skala hvor full identifiserbarhet er motsetningen. Midt i mellom finner vi *pseudonymitet* som lar brukere av elektronisk kommunikasjon opptre med fiktive og virtuelle identiteter. Samtidig finnes det, avhengig av løsningen, sterke eller svake koplinger til den reelle brukeren bak slik at samfunnets behov for identifisering blir ivaretatt ved behov. Man vil dermed kunne være anonym overfor de man kommuniserer med. Pfitzmann og Hansen lister opp ulike typer av pseudonymer som kan brukes i elektronisk kommunikasjon, som vist i figur 14.



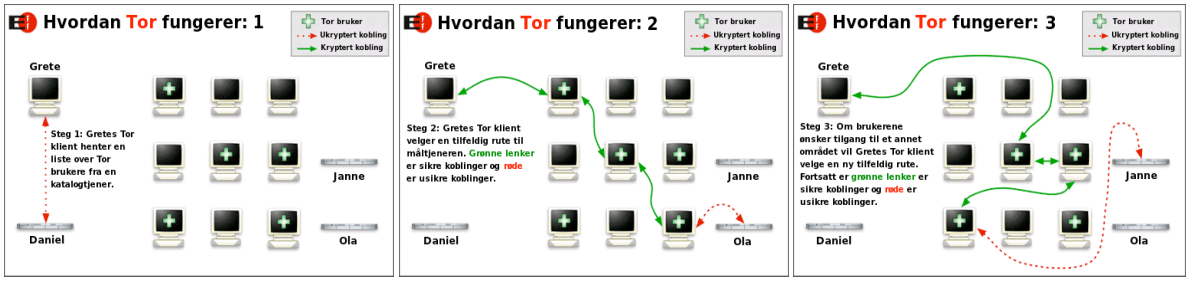
Figur 38: Grad av anonymitet i pseudonymer (Pfitzmann & Hansen 2005, side 18)

De ulike pseudonymene tilbyr ulik grad av anonymitet, og i figuren vil pseudonymene tilby mer og mer anonymitet jo lenger ned mot bunnen man kommer. Et *personpseudonym* er et substitutt for en sivil identitet, og kan være et personnummer eler et telefonnummer. Personpseudonym representerer liten grad av anonymitet da slike opplysninger er offentlig tilgjengelige og dermed relativt enkle å koble til et individ. Et *rollepseudonym* er knyttet til en spesifikk rolle, som for eksempel kan være en rolle som kunde representert med et kundenummer eller rollen som internettbruker representert gjennom en IP-adresse. Et *relasjonspseudonym* representerer et individ i kommunikasjon med andre og kan være et spesifikk kallenavn man bruker i et nettsamfunn. *Rolle-relasjonspseudonym* representerer også et individ i kommunikasjon med andre men denne gangen med ulike pseudonym for ulike roller. På den måten vil ikke en kommunikasjonspartner kunne kartlegge bevegelsene til individet bak det gitte pseudonymet fordi denne ikke vil kunne vite hvorvidt det samme pseudonymet i en annen rolle tilhører samme individ. Et *transaksjonspseudonym* vil være representert gjennom et transaksjonsnummer. Slik et kjøp i en butikk genererer en kvittering med et nummer generer også netthandel slike uten at kunden i prinsippet skulle trenge å identifisere seg. Transaksjonspseudonym representerer en svært svak kopling til et individ.

5.2.3 Bruk av personvernøkende teknologi

Personvernøkende teknologi kan benyttes både i tjenestelaget og i kommunikasjonlaget. (NOU 2009:1, side 284) Kommunikasjonslaget er den tekniske infrastrukturen og handler om identifisering av maskiner mens det i tjenestelaget handler om identifisering og autentisering av brukere.

Informasjonskapsler (cookies) og IP-adresse gjør det mulig for en tjenesteyter å gjengkjenne en bruker. I tilfeller hvor brukeren har fast IP-adresse vil det være mulig å generere profil over IP-adressers bruksmønstre. Dersom brukeren identifiserer seg ved en senere anledning vil bruksmønsteret kunne knyttes til IP-adressen for senere bruk. For å hindre dette finnes det tekniske løsninger bruker kan benytte seg av som undertrykker brukerens reelle adresse og genererer nye slik at brukeren ikke kan knyttes til den. Slike tjenester bygger på ruting via proxyservere, som er en server brukeren kan gå via for å etablere kontakt med tjenesteleverandører. Proxyserveren gir brukeren ny IP-adresse og fjerner dermed koblingen som finnes hos internettleverandøren. Et eksempel på en tjeneste som bruker slik teknologi er det norske TOR nettverket, som ved å sende datatrafikken gjennom et tilfeldig mønster gjør det umulig å spore tilbake til avsenderen. Nettverket er bygd opp ved at frivillige rundt omkring i hele verden installerer et lite program som gjør at deres maskin blir brukt som en proxy i nettverket. Når du bruker TOR sendes datatrafikken din gjennom tre slike, og ingen av dem vet hele ruten mellom deg og destinasjonen. På denne måten kan brukeren opptre fullstendig anonymt[42] med mindre brukeren selv identifiserer seg overfor andre.



Figur 39: TOR-netteverket[43]

Informasjonskapsler er små tekstfiler tjenesteyter lagrer på en brukers maskin som inneholder transaksjonshistorikken mellom nettleser og webserver. Dette er funksjonalitet som ikke ligger i internetts arkitektur fra før og er en viktig ingrediens ved for eksempel netthandel for at tjenesteyter skal kunne holde rede på hvilke varer brukeren har lagt i handlekurven sin. Disse kan imidlertid også brukes til å bygge profiler av brukere, og kan komme i form av typer uønsket programvare som jeg har sett på i kapittel 4. Brukeren har imidlertid flere tekniske løsninger å velge mellom for å kontrollere tjenestens adgang til å plassere informasjonskapsler på sin maskin. Blant annet er dette innebygget som standard i de mest utbredte nettleserne på markedet. Også i kommunikasjon mellom bruker og tjenesteyter i tjenestelaget kan PETs brukes for å ivareta personvernet. Et mye

[42] Les mer om TOR-nettverket: http://www.torproject.org/overview.html.no

[43] www.torproject.org/overview.html.no

brukt eksempel er P3P (Platform for Privacy Preferences) som muliggjør at brukere og tjenestetilbydere kan utveksle personvernpreferanser. Programmet oppretter en dialog med en tjenestetilbyder og gir beskjed til brukeren dersom denne har en personvernpolicy som ikke er i samsvar med brukerens egne preferanser.

5.2.3 Samlet vurdering

Som et tiltak mot identitetstyveri bør det av både offentlige og private tilbydere legges opp til muligheter for anonym eller pseudonym opptreden på nett i de tilfeller hvor identifisering ikke er nødvendig. På denne måten vil man kunne redusere tilgjengeligheten til personopplysninger og dermed også farene for identitetstyveri, fordi fravær av personopplysninger betyr at det ikke finnes opplysinger som kan misbrukes. Tekniske løsninger bør derfor i større grad legge opp til bruk av ulike pseudonymer for å unngå bruk av personopplysninger i den grad det er mulig.

Resonnementet fungerer imidlertid dårlig for identitetstyveri av fiktive og virtuelle identiteter. Det er heller langt fra alle situasjoner hvor det er ønskelig eller mulig å kunne opptre fullstendig anonymt. Et annet teknisk tiltak jeg skal se på er derfor personvernøkende identitetsforvaltning, som på mange måter forsøker å kombinere samfunnets behov for identifisering med den enkeltes rett på anonymitet. Slike løsninger adresserer trusler knyttet både til opplysningers konfidensialitet og integritet og spørsmål knyttet til autentisering av brukere. Anonymitet og pseudonymitet kan løse problemene ved å *ta bort verdiene*, personvernøkende identitetsforvaltning ønsker derimot å bruke sterke mekanismer til å *sikre verdiene*.

5.3 Personvernøkende identitetsforvaltning som tiltak

Elektronisk identitetsforvaltning ble i kapittel 4 behandlet som en trussel for den enkeltes personvern. Dette fordi utstrakt innsamling og behandling av personopplysning i løsninger uten tilstrekkelig sikkerhet utgjør en fare for identitetstyveri. Elektronisk identitetsforvaltning er imidlertid ikke ett konsept med én definisjon og én løsning, men heller et sett med ulike modeller. Det kan derfor tenkes at elektronisk identitetsforvaltning ikke bare er en del av problemet men også en del av løsningen. I følge Olsen og Mahler (Olsen & Mahler 2005, side 55) kan man skille mellom fire modeller.

- Brukerstyrt identitetsforvaltning
- Enkeltorganisasjon Single Sign-On
- Flerorganisasjon Single Sign-On

- Føderert identitetsforvaltning

Brukerstyrt identitetsforvaltning[44] er løsninger hvor brukeren håndterer sin elektroniske identitet gjennom lagring lokalt i egnede applikasjoner eller via internett hos en tredjepart. Det fleste nettlesere gir i dag brukerne mulighet for å lagre identifikator og autentifikator dersom autentiseringsmekanismen ikke selv inneholder en sperre mot slik lagring. Disse applikasjonene fyller også inn disse automatisk for brukeren hver gang han besøker en tjeneste hvor dette valget er foretatt. Løsningene omtalt i kapittel 4 ligger i denne kategorien, og er dermed relativt enkle applikasjoner for tilgangsstyring og håndtering av elektroniske identiteter.

Enkeltorganisasjon Single Sign-On (SSO) er løsninger som girt brukeren mulighet til å aksessere flere tjenester fra samme tjenesteleverandør men med kun én innlogging. Slike løsninger finner man ofte i jobbsammenheng hvor ansatte blir gitt tilgang til flere ulike løsninger med samme innlogging.

Flerorganisasjon Single Sign-On (SSO) gir brukeren tilgang til tjenester på tvers av organisasjonsplattformer. Slike løsninger er brukervennlige fordi det blir færre identifikatorer og autentifikatorer for brukeren å huske, og kan også være kostnadseffektivt fordi identitetsforvaltningen kan settes bort til spesialiserte tredjeparter. Identitetstilbyderen vil kun autentisere brukeren mens tjenesteleverandøren vil autorisere og gi brukeren tilgang til riktige ressurser innenfor organisasjonen.

Føderert identitetsforvaltning tilbyr på samme måten tjenester på tvers av organisasjonsplattformer, men er i tillegg en underliggende teknologi som også gjør det mulig for brukere å benytte seg av flere ulike identitetstilbydere. Eksempler på føderert identitetsforvaltning finner vi i FEIDE som tilbyr nasjonal elektronisk identitet i utdanningssektoren. Ifølge Olsen og Mahler er en populær definisjon av føderert identitetsforvaltning ”the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains”. (Olsen og Mahler 2005, side 59) Føderert identitetsforvaltning er altså underliggende protokoller som muliggjør utveksling og håndtering av identitetsdata på tvers av både tjenestetilbydere og identitetstilbydere.

Fokuset videre er føderert identitetsforvaltning og om slike løsninger vil kunne bidra til økt personvern i elektronisk identitetsforvaltning.

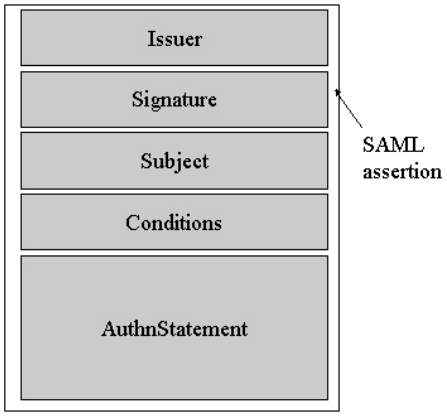
[44] Internasjonalt omtalt som *user centric*.

5.3.1 Tekniske løsninger for føderert identitetsforvaltning

Den tekniske standarden som ligger til grunn for flere løsninger for føderert identitetsforvaltning er den åpne XML baserte standarden SAML 2.0. Blant løsningene som bruker standarden finner vi norske eksempler i MinID og FEIDE. Standarden definerer et meldingsformat for hvordan brukerinformasjon gjennom såkalte *assertions* kan utveksles mellom ulike aktører, og hvordan aktører kan *forespørre* og *respondere* (response-request) på slike *assertions*. Direkte oversatt betyr assertion påstand, og refererer dermed til å komme med en *påstand* om brukeridentitet. SAML definerer videre hvordan aktører kan referere til den samme bruker på tvers av organisasjonsplattformer ved å etablere en *felles føderert identifikator*. Føderert identitetsforvaltning tilbyr i tillegg til føderering av identitet også funksjonalitet for SSO og Single-Log-Out (SLO). På samme måte som SSO funksjonalitet gjør det mulig å bevege seg mellom tjenester og tjenesteleverandører med bare én innlogging gjør SLO funksjonalitet det mulig for brukeren å logge ut på samme måten. Jeg skal i det videre fokusere på føderering av identiteter samt personvern knyttet til autentisering og konfidensialitet i en modell for føderert identitetsforvaltning.

5.3.1.1 Komponenter i SAML 2.0

SAML består av flere komponenter som til sammen utgjør en arkitektur for utveksling av identitetsdata på tvers av tekniske og organisatoriske plattformer. Påstandene er standardiserte og angir hvem som er utsteder, utsteders signatur, informasjon om subjektet, vilkår for bruk og informasjon om hvordan brukeren ble autentisert.



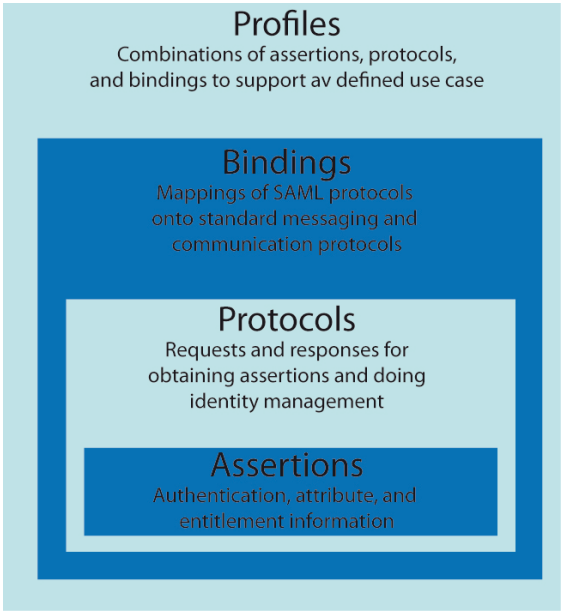
Figur 40 Oppbyggingen av en påstand (OASIS 2005, side 4)

Påstandene kan uttrykke tre typer erklæringer:

- *Autentisering*: erklæring om når og av hvem ble brukeren autentisert

- *Attributter*: erklæring om at brukeren er assosiert med attributter som følger med påstanden
- *Autorisasjon*: svar på spørsmål om tilgang blir enten bekreftet eller avkreftet.

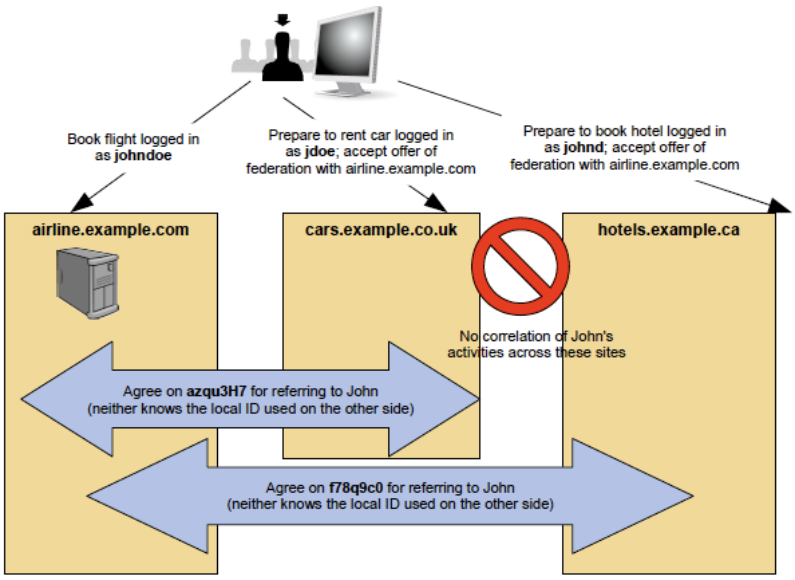
Påstandene utveksles ved hjelp av response-request protokoller, som sammen med påstandene utgjør kjernen i standarden. Det er også to andre hovedkomponenter i SAML, som sammen med påstandene og protokollene utgjør arkitekturen til SAML. Dette er *SAML bindings* som definerer hvordan SAML protokollene kan transporteres til mottaker ved å knytte dem til underliggende transportprotokoller som HTTP eller andre lignende protokoller. *SAML profiles* er ferdige kombinasjoner av de tre andre komponentene for å støtte de vanligste bruksformål.



Figur 41: Komponenter i SAML 2.0 (OASIS 2005b, side 10)

En av de viktigste komponentene og en forutsetning for mange av de sentrale tjenestene som finnes i SAML er opprettelsen av en felles føderert identifikator for å referere til felles brukere. En slik identifikator kan brukes til å linke eksisterende brukerkontoer eller opprette nye med utgangspunkt hos en identitetsforvalter. Figuren under viser et eksempel på føderering av eksisterende brukerkontoer, hvor *airline.example.com* er identitetsforvalter mens *cars* og *hotels* er tjenesteleverandører. Brukeren er her kjent med ulike identifikatorer hos de ulike tjenesteleverandørene som han allerede har brukerkonto hos, hhv. johndoe, jdoe og johnd. I prosessen med å føderer brukerkontoene blir identitetsforvalteren enig med tjenesteleverandøren om hvilken felles identifikator brukeren skal være kjent under. Tre ulike identifikatorer med ulike egenskaper kan benyttes: (OASIS 2008, side 38)

- Vedvarende pseudonym som er knyttet til den lokale identifikatoren hos både identitetstilbyderen og tjenestetilbyderen.
- Midlertidig pseudonym som kun brukes for én sesjon og dermed hindrer en tjenesteleverandør å gjenkjenne tilbakevendende brukere.
- Et brukerattributt som kundenummer, e-mail og lignende.



Figur 42: Føderering av brukerkontoer (OASIS 2008, side 14)

Bruk av pseudonym, og da fortrinnsvis ulike pseudonym for ulike tjenesteleverandører, er valgt av personvernhensyn. (OASIS 2008, side 24) Dette vanskeliggjør samkjøring av informasjon mellom tjenesteleverandører, som i figuren representeres med et stopptegn, utover linken som finnes til identitetstilbyder. Dette er likevel ikke til hinder for samkjøring av opplysinger tilknyttet de lokale identifikatorene. Dette skyldes imidlertid ikke arkitekturen til SAML, men heller hva brukeren har oppgitt av informasjon selv.

Attributtautentisering åpner opp for å ikke identifisere identitet men heller andre egenskaper ved en bruker. Ved on-line filmleie vil det for eksempel være irrelevant hvem brukeren er så lenge denne er gammel nok til å leie filmen. Slik utveksling gjør det også mulig for brukeren å opprette brukerkontoer hos tjenesteleverandører ved å utveksle hele brukerkontoer eller et gitt antall attributter. FEIDE har implementert dette i sin løsning som jeg skal komme tilbake til i neste avsnitt.

Det finnes videre mekanismer i teknologien som gjør det mulig for brukeren og tjenestetilbyderen å kommunisere vilkår for bruken av opplysningene. Dette er illustrert som *Condtions* i figur 16 over. Dette elementet angir detaljer vedrørende erklæringens gyldighet i tid, restriksjoner, adgang til videre bruk osv. SAML støtter også kryptering. Dette gjelder både for deler av en påstand eller for hele, avhengig av behov. Dette er med å sikrer konfidensialiteten og integriteten kommunikasjonen av identitetsdata.

SAML er dermed å forstå som en underliggende arkitektur som muliggjør føderert identitetsforvaltning og flerorganisasjons SSO gjennom å tilby en kommunikasjonsplattform for utveksling og håndtering av identitetsdata. Slik TCP/IP er protokoller som muliggjør elektronisk kommunikasjon mellom datamaskiner i et nettverk er altså SAML protokoller som muliggjør kommunikasjon av identitetsdata på tvers av organisasjoner og plattformer.

Personvernhensyn har ifølge utviklerne i OASIS[45] vært delvis førende for utviklingen av standarden. I hvilken grad personvernet blir tatt hensyn til er imidlertid opp til identitetsforvaltere og tjenestetilbydere fordi arkitekturen tilbyr ulike valg som disse selv må velge å bruke. Jeg skal videre se hvordan de offentlige prosjektene for eID MinID og FEIDE har implementert SAML 2.0 i sin arkitektur.

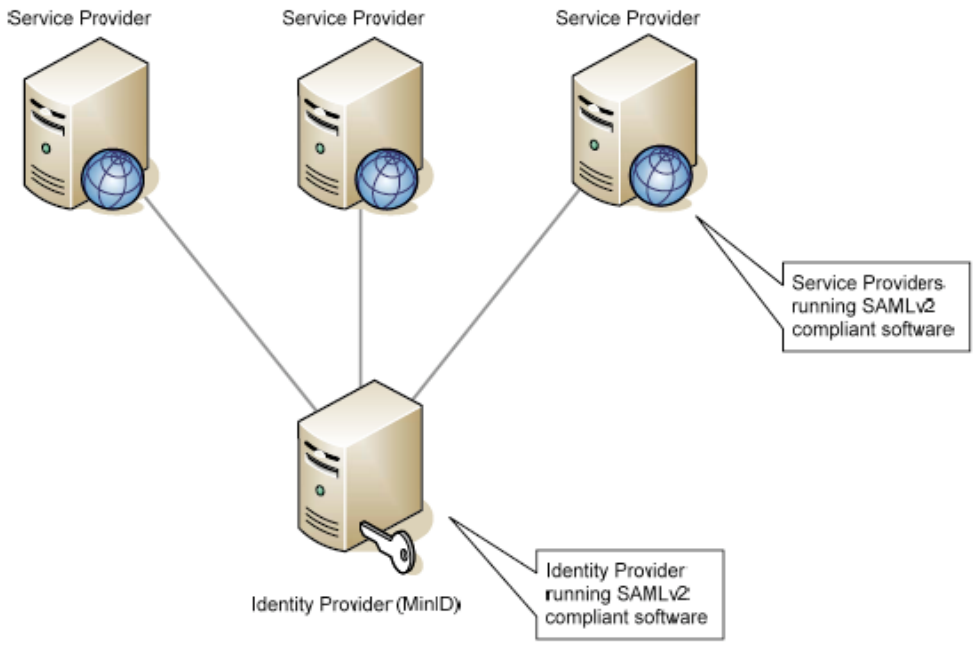
5.3.2 Eksempel på bruk av føderert identitetsforvaltning i MinID og FEIDE

MinID tilbyr flerorganisasjons[46] SSO funksjonalitet for autentisering av brukere i elektronisk kommunikasjon med det offentlige. MinID fungerer i dag som autentiseringsløsning opp mot flere offentlige tjenester, inkludert MinSide, folkeregisteret (via MinSide) og Lånekassen, og kan også brukes for å melde adresseendring hos Posten. MinID gir dermed tilgang til mye av informasjonen det offentlige har registrert på hver enkelt av oss. Informasjonen ligger hos hver enkelt etat, men er også tilgjengelig for brukerne gjennom borgerportalen MinSide. MinSide tilbyr *transaksjonstjenester* og *registertjenester*. Transaksjonstjenester er lenker i MinSide som sender brukeren til andre tjenester som bruker MinID som autentiseringsløsning. For eksempel kan man bestille nytt skattekort via MinSide, men den faktiske bestillingen gjennomføres ved at brukeren

[45] Organization for the Advancement of Structured Information Standards

[46] Behandlingsansvaret i det offentlige er delt mellom departementene og etatene, derfor er løsningen flerorganisasjons SSO. (Moderniseringsdepartementet 2005b, side 11)

blir videresendt til den aktuelle tjenesten. Registertjenester er når MinSide gjør oppslag i etatenes egne registre og presenterer dataene for brukeren, slik som oppslag i folkeregisteret eller skatteetaten. Figuren under illustrerer sammenhengen mellom MinID som identitetstilbyder (Identity Provider) og ulike tjenesteleverandører (Service Providers) inkludert MinSide.



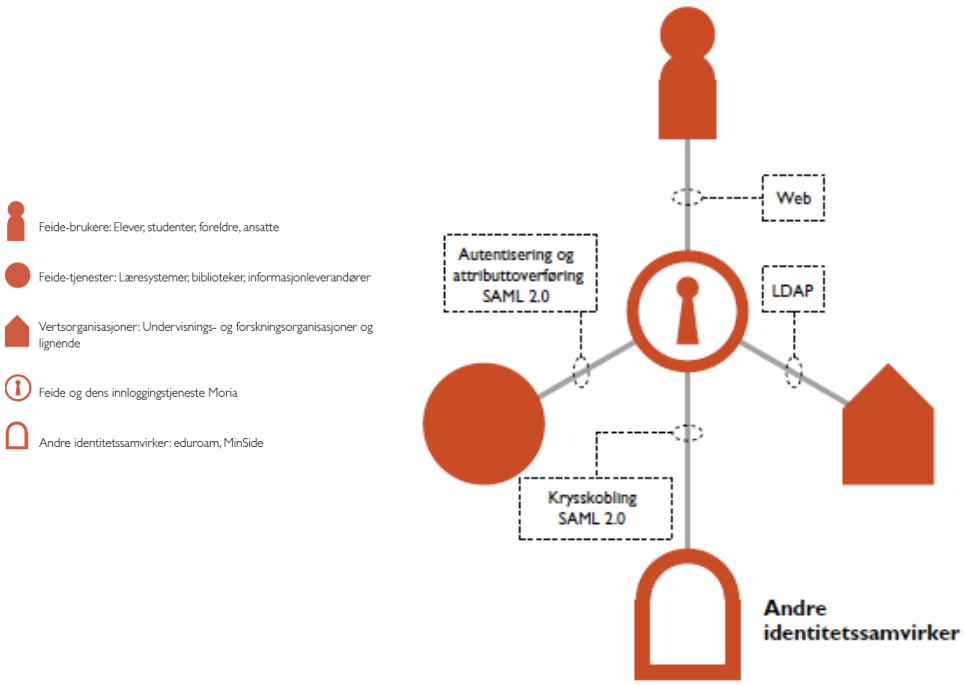
Figur 17: Sammenhengen mellom MinID og tjenesteleverandørene(Software Innovation 2006, side 5)

FEIDE[47] er et nasjonalt tiltak for enhetlig identitetsforvaltning i utdanningssektoren for både studenter og ansatte, og fungerer som en sentral innloggingstjeneste hvor brukere blir autentisert og gitt tilgang til lokale tjenester. FEIDE er bygd opp med

- Brukere
- Vertsorganisasjoner
- Tjenesteleverandører

Brukerne er alle studenter eller ansatte, vertsorganisasjonene er de som har brukerinformasjon lagret hos seg, og tjenesteleverandørene er de som leverer tjenester og har behov for å autentisere brukerne for innlogging. Dette kalles for FEIDEs identitetssamvirke.

[47] **F**elles **E**lektronisk **IDE**ntitet



Figur 18: Komponenter og grensesnitt i FEIDEs identitetssamvirke (FEIDE systemarkitektur, side 17)

5.3.2.1 Føderering av identitet

Det er lagt opp til at enheter kan knytte seg til MinID gjennom det man kaller *circle of trust*. Dette er en betegnelse som brukes om den gruppen av tjenesteleverandører som er tilknyttet identitetstilbyderen og hvor brukerne får tilgang på tjenester gjennom autentiseringen hos identitetsforvalter. Føderering av identitet gjennom MinID skjer ved at opplysninger på tvers av offentlige organ blir koplet sammen og gitt tilgang til gjennom én innlogging. Fødereringen skjer automatisk når brukeren registrerer seg som bruker av MinID. MinID er en sentralisert løsning med tanke på lagring av personopplysninger.

FEIDE realiserer føderering av identitet gjennom avtaler med identitetsforvaltere dersom disse opererer med autentisering på sikkerhetsnivå som er sammenliknbart med FEIDE. (FEIDE systemarkitektur, side 15) Dette innebærer at også identitetsforvalteren må basere seg på SAML 2.0 slik at tjenestene kan kommunisere med hverandre. Også her er det stor grad av auto-føderering ved at tjenester som har avtaler med FEIDE og som brukeren skal ha tilgang til blir koblet sammen automatisk.

5.3.2.2 Autentisering av brukere

MinID autentiserer brukere ved hjelp av både pinkoder, selvvalgt passord og fødselsnummer. Pinkodene blir sendt til folkeregistrert adresse og fungerer som autentisering ved førstegangspålogging. I denne prosessen oppretter brukeren et selvvalgt passord som sammen med pinkodene benyttes ved senere autentisering. Pinkodene har man tilgjengelig på kodekortet man får tilsendt til folkeregistrert adresse, men man kan også velge å få engangskoder tilsendt på SMS hver gang man skal logge inn. MinID er en sentralisert autentiseringsløsning ved at brukerdatabasen er en sentral LDAP katalog. Dette er en standardisert katalogtjeneste, eller noe som er litt mer spesialisert enn en database, og som inneholder informasjon om personer.

I FEIDE blir brukernavn og passord tildelt brukerne fra deres lokale institusjon, og opplysninger om brukerne lagres i lokale LDAP kataloger kontra sentralt slik det gjøres i MinID. De lokale LDAP katalogene kan samlet sett ses på som én stor distribuert database. (FEIDE systemarkitektur, side 20) I praksis fungerer FEIDE slik at brukeren aksesserer websiden til den tjenesten han ønsker å bruke og logger inn med sin elektroniske identitet utstedt fra sin egen organisasjon. Dette blir returnert til FEIDE som igjen videresender denne til vertsorganisasjonens lokale FEIDE katalog for kontroll. Vertsorganisasjonen returnerer deretter bekreftelse på autentisering til FEIDE samt de attributter som er registrert på brukeren. Til sist sender FEIDE denne bekreftelsen samt de attributter som tjenesten har avtale om at skal utleveres. Tjenesteleverandørene får dermed kun tilgang til attributter om en bruker som er regulert i avtale, og er dermed behovsbasert.

Autentiseringsløsningene som benyttes i begge tjenestene er passord som kun aksepterer kombinasjoner av bokstaver og tall samt minimum 8 tegn.

5.3.2.3 Uveksling av personinformasjon

Autentisering av brukere i MinID skjer på individnivå, og fødselsnummer er derfor en del av påstanden som overføres mellom MinID og tjenesteleverandør. I den formen MinID er i dag er det imidlertid svært lite personopplysninger lagret i den elektroniske identiteten. Opplysningene som er lagret er knyttet til *påstanden* som sendes til brukerstedene: fødselsnummer, språkvalg og sikkerhetsnivå. Noen opplysninger er knyttet til brukerprofilen, slik som telefonnummer og e-post adresse dersom brukeren har registrert dette. Andre opplysninger knyttet til en identitet gir MinID tilgang til ved autentisering, men opplysningene lagres hos den enkelte etat eller departement.

Attribute	Value	Example
uid	Social security number (fødselsnummer), 11 digits	01020312345
Culture	language-code[-/_country-code]	nb nb-NO nb_NO
SecurityLevel	one digit	3

Figur 43: Påstand i MinID (Software Innovation 2006, side 9)

Utveksling av personinformasjon i FEIDE er regulert i avtaler mellom FEIDE og tjenesteleverandør og mellom FEIDE og vertsorganisasjonene. Om identifikasjon og utlevering av personopplysninger til de ulike aktørene oppgir FEIDE som følger:

”I utgangspunktet kjenner ikke tjenesteleverandører brukerens Feide-navn, kun en *koblingsnøkkel* som ikke gir informasjon om brukeren. Etter avtale med Feide kan et utvalg brukerattributter overføres ved innlogging, i den grad det er nødvendig for å utføre tjenesten. Koblingsnøkkelen kan brukes f.eks. til å identifisere en personlig profil lagret i tjenesteleverandørens system, en lokal konto eller for lokal tilgangskontroll. En bruker har forskjellig koblingsnøkkel for hver tjeneste, og man kan ikke koble informasjon fra ulike tjenesteleverandører om samme bruker på grunnlag av koblingsnøkkelen.

Enkelte attributter, f.eks. fødselsnummer, identifiserer en person unikt, og kan brukes til å koble informasjon fra ulike kilder. Også andre attributter, f.eks. e-postadresse, gir nær entydig personidentifikasjon. Feide er restriktiv med hensyn på å gi tilgang til attributter som identifiserer enkeltpersoner, og tjeneste-leverandører må vise til et reelt behov for å få utlevert disse gjennom Feide.” (FEIDE systemarkitektur, Side 8)

Attributter om personer i FEIDE er:

Attributter om personer

Informasjonselement (obligatorisk)	Attributtnavn
Feide-navn	eduPersonPrincipalName
Lokal brukeridentitet	uid
Passord	userPassword
Epostadresse	mail
Etternavn	sn
Fornavn	givenName
Foretrukket navneform	displayName
Fødselsnummer	norEduPersonNIN
Tilknytning til organisasjonen	eduPersonAffiliation
Rettighet	eduPersonEntitlement
Tilknytning til organisasjon, med detaljer om organisasjon	eduPersonScopedAffiliation
Fullstendig navn på personobjekt i LDAP	cn
Peker for å slå opp organisasjonsinformasjon	eduPersonOrgDN
Peker til organisasjonsenhet	eduPersonOrgUnitDN

Figur 44: Attributter i FEIDE[48]

5.3.2.4 Sikring av konfidensialitet

Sikring av konfidensialitet skjer på to områder: sikring av transportdata og sikring av lagrede opplysninger. Transportdata er informasjonen som flyter mellom serverne til tjenesteleverandør og identitetsleverandør samt kommunikasjonen fra disse til brukerens nettleser.

MinID benytter seg av SSL sertifikat med trippel DES 168 bit høygradskryptering. DES er forkortelsen for *Data Encryption Standard* som er en krypteringsalgoritme med en krypteringsnøkkel på 56 biter. At den er trippel betyr videre at DES algoritmen brukes 3 ganger noe som gir en krypteringsnøkkel på 168 biter. Ifølge Sun Microsystems er dette den sterkeste SSL krypteringen per i dag[49]. På denne måten sikrer man at uvedkommende har mulighet til å snappe opp informasjonen som blir kommunisert mellom servere og mellom servere og nettleser. Vi snakker her om *transportsikring* av informasjonen.

FEIDE benytter seg også av SSL sertifikat, men benytter seg av Camellia-256, i likhet med Facebook, jf. kapittel 4. Det finnes ingen offentlig tilgjengelige kilder angående hvordan tjenestene beskytter lagrede data. Som nevnt i forrige avsnitt Med FEIDE og MinID som tekniske rollemodeller er Fornyings- og Administrasjonsdepartementet i gang med å planlegge en arkitektur for utveksling og håndtering av identitetsdata bygget på SAML 2.0. Jeg skal se kort hva arkitekturen går ut på og hvilke muligheter som ligger der i et langsiktig perspektiv.

[48] http://feide.no/content.ap?thisId=8724

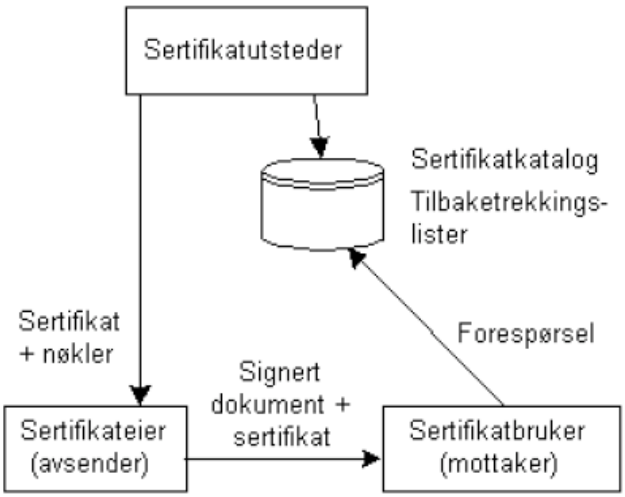
[49] http://docs.sun.com/source/816-6156-10/contents.htm

5.3.3 Eksempel på bruk av føderert identitetsforvaltning i arkitektur for håndtering og utveksling av identitetsdata

Arkitekturen består av en teknisk infrastruktur for bruk av eID opp mot offentlig sektor og et rammeverk som angir hvor sterk autentisering ulike offentlige løsninger har behov for. Arkitekturen er videre ment som en videreføring av arbeidet gjort med MinID.

5.3.3.1 eID og autentisering i offentlig sektor

Offentlig utstedt eID er planlagt å være digitale sertifikater bestående av krypterte offentlige og private nøkler samt en digital signatur. Teknologien tenkt benyttet er PKI (Public Key Infrastructure), en infrastruktur for utstedelse, administrasjon og bruk av digitale sertifikater. I en PKI kan digitale sertifikater brukes til å identifisere deg for å få adgang til beskyttet info og til å signere digitale dokumenter ved benytte seg av krypterte nøkler: en privat nøkkel som kun brukeren kjenner og en som er allment og offentlig tilgjenglig. Disse nøklene bindes så sammen av en sertifikatutsteder som bekrefter en gitt brukeridentitet. En digital signatur er et dataelement som blir lagt til en elektronisk melding som binder et dokument til en elektronisk ID.



Figur 45: Elementer i en PKI (NOU 2001:10, side 24)

Signaturen blir unikt fremstilt på bakgrunn av innholdet i et dokument. Dersom dokumentet er blitt endret fra det er blitt kryptert og signert og frem til mottaker dekrypterer vil ikke signaturen som mottaker fremstiller lenger matche den som avsender sendte med. Nøklene skal beskyttes med pinkoder (Politi- og Justisdepartementet 2007, side 57), og ifm. at offentlig utstedt eID er foreslått realisert sammen med nasjonalt id-kort trenger brukeren også en kortleser. (Politi- og Justisdepartementet 2007, side 58)

Rammeverk for autentisering og uavviselighet er å forstå som angivelser på sikkerhetsnivå for å sikre at i) riktig person blir autentisert med riktig identitet og ii) at informasjonen i dialogen ikke skal kunne endres uautorisert[50]. Fire sikkerhetsnivå er definert i rammeverket ut fra konsekvenser ved sikkerhetsbrudd. Desto større konsekvensene blir ved sikkerhetsbrudd desto høyere sikkerhetsnivå vil en gitt elektronisk løsning ha behov for. (Fornyings- og Administrasjonsdepartementet 2007, side 77) Mest usikkerhet er det knyttet til sikkerhetsnivå 3 og 4 som krever sterke mekanismer for sikkerhet og autentisering. Offentlig utstedt eID er ment å tilfredsstille kravene til sikkerhetsnivå 4.

- **Sikkerhetsnivå 3**

  Løsninger som benytter seg av
  - passordkalkulator med pinkode der første koden blir sendt i separat forsendelse,
  - engangspassord på mobiltelefon der mobiltelefonen er registrert med en egen registreringskode distribuert til folkeregistrert adresse ,
  - person Standard iht. Kravspesifikasjon for PKI i offentlig sektor eller
  - engangspassordlister benyttet sammen med fast passord og brukernavn. Valg av fast passord skal skje på bakgrunn av en engangskode sendt til folkeregistrert adresse (eventuelt første kode på engangspassordlisten).
- **Sikkerhetsnivå 4**
  - En tofaktorløsning, hvor en av faktorene er dynamisk, hvorav en av faktorene eller en registreringsfaktor er personlig utlevert. Det benyttes en tredjepart til å registrere en logg med knytningen mellom handling/ informasjonselement og identitet. Loggen skal lagres med endringsbeskyttelse.
  - Eller en tofaktorløsning, hvor en av faktorene er dynamisk, hvorav en av faktorene eller en registreringsfaktor er personlig utlevert. Det benyttes en spesialprogramvare som hindrer brukersted i å generere falsk dokumentasjon over hvem som står bak et informasjonselement/handling og som hindrer operatører å kunne endre logging av informasjonselement/ handlingsbeskrivelse og identitet.

[50] Uavviselighet = informasjonsintegritet, for å bekrefte at en handling eller et informasjonselement er uendret og at det kan knyttes til en bestemt identitet. (Fornyings- og Administrasjonsdepartementet 2007, side 77)

Rammeverket er kun en veiledning som gir anvisninger og anbefalinger, det er opp til hver enkelt institusjon å selv foreta risikoanalyser og vurderinger for deretter å plassere sine løsninger på riktig nivå.

5.3.3.2 Felles infrastruktur for eID i offentlig sektor

Felles infrastruktur for eID har som hovedformål å muliggjøre håndtering og utveksling av identitetsdata på tvers av organisasjonsplattformer både i det offentlige og det private. Infrastrukturen har videre som hensikt å tilrettelegge for flere tilbydere av eID, ikke bare offentlig utstedt gjennom nasjonalt id-kort men også fra godkjente markedsleverandører. Infrastrukturen er dermed ment å koble sammen ulike identitetsleverandører med tjenestetilbydere og er ment å være offentlig forvaltet. Infrastrukturen skal støtte en rekke tjenester, blant annet autentisering og videreformidling av eID, digital signering av webskjema og generell støtte for kryptering. (Fornyings- og Administrasjonsdepartementet 2007, side 17)

Både nåværende og planlagte løsninger for eID og identitetsforvaltning baserer seg på bruk av typer av passord eller pinkoder for autentisering av brukere. Autentisering er imidlertid ikke noe som bestemmes i arkitekturen til SAML, utover hvordan man skal identifisere brukere overfor tjenesteleverandører. Slike autentifikatorer er imidlertid ikke knyttet til et individ på annen måte enn at det er noe individet vet eller har. Biometriske mønstre er derimot kjennetegn som er uløselig knyttet til et individ og som ved hjelp av biometriske system kan brukes til autentisering av brukere. Slike kan derfor tenkes brukt for sikker autentisering opp mot offentlig eID, noe jeg kommer tilbake til i avsnitt 5.4.

5.3.3.3 Føderert identitetsforvaltning som identitets infrastruktur i samfunnet?

Innføring av en felles infrastruktur kan slik jeg vurderer det sies å ha både kortsiktige og langsiktige formål. Kortsiktig legger infrastrukturen til rette for at både private aktører og offentlige utstedere av eID skal kunne tilby eID opp mot offentlige tjenester for å sikre rask utbredelse av eID på sikkerhetsnivå 3 og 4. På lang sikt kan infrastrukturen gjennom å bygge på SAML 2.0 ha et formål som knutepunkt for kommunikasjon av identitetsdata mellom identitetstilbydere og tjenesteleverandører i samfunnet som helhet.

Arkitekturen departementet jobber med virker å være fremtidsrettet i den grad SAML 2.0 er en åpen standard med mange muligheter. Arkitekturen kan bygges gradvis og har potensialet til å bli en

identitets infrastruktur i samfunnet dersom man bruker mulighetene som ligger der. Det er imidlertid langt frem til dette eventuelt kan bli en realitet. Mange hensyn skal tas, og det er ikke gitt at personvernhensyn vinner frem. Som tilrettelegger for sikrere håndtering og utveksling av identitetsdata er arkitekturen departementet foreslår imidlertid en spennende satsning. Det samme gjelder autentisering av brukere som gjennom bruk av krypterte digitale sertifikater og signaturer gjør det svært vanskelig å kunne opptre med en annens identitet.

5.3.4 Samlet vurdering

Personvernøkende identitetsforvaltning gjennom løsninger for føderert identitetsforvaltning adresserer en rekke av de truslene som ble identifisert i kapittel 4. Sikring av personopplysningers konfidensialitet og integritet ivaretas gjennom krypterte forbindelser mens autentiseringsproblematikken blir forsøkt løst ved å ta i bruk både sikrere og flere ulike autentifikatorer. Føderert identitetsforvaltning muliggjør videre både sterk autentisering og pseudonym kommunikasjon med tjenesteleverandører ved at en bruker kan identifisere seg hos en tiltrodd identitetsforvalter mens senere kommunikasjon med tjenesteleverandører kan gjøres ved bruk av pseudonym. Samfunnet vil på denne måten få tilfredsstilt sitt behov for identifisering ved at brukerens identitet ved behov kan utleveres[51], samtidig som brukeren vil være anonym overfor den andre part.

Fordelene med føderert identitetsforvaltning er den potensielle kombinasjonen av personvernøkende elementer og sterk sikring og autentisering. Ulempene er derimot at løsningene potensielt gir tilgang til svært mye informasjon om hver enkelt bruker, og dermed innebærer svært negative konsekvenser dersom sikkerhetsmekanismene ikke er tilstrekkelige. For brukerne er det både enklere og sikrere å forholde seg til én innlogging. Dermed unngår mange lange og kompliserte passord som gjerne fører til at disse blir notert ned på papir eller i et elektronisk dokument. Selv om det ikke finnes noen garanti for hva den enkelte bruker faktisk velger å gjøre vil risikoen uansett reduseres. Det samme gjelder for de begrensninger og føringer som pålegges brukeren i form av lengde og form på passord samt at det ikke er mulig for brukeren å eksponere sin elektroniske identitet gjennom lagring i nettleser. Gjennom å benytte dynamiske autentiseringsfaktorer slik MinID gjør er det også nødvendig å være i fysisk besittelse av brukerens pinkoder eller det mediet brukeren får tilsendt slike pinkoder til ved pålogging. Dette må kunne

[51] Eksempelvis gjennom rettslig kjennelse om utlevering slik vi i dag kjenner det fra saker om utlevering av IP-adresser.

anses som en vesentlig faktor for å redusere truslene knyttet til autentisering. Samtidig er det et viktig poeng at autentiseringsmekanismer ikke er en del av arkitekturen til føderert identitetsforvaltning. MinID og FEIDE benytter eksempelvis helt forskjellige autentiseringsløsninger. FEIDEs én-faktor autentisering representerer ingen sikker løsning, mens MinID foreløpig kun er på sikkerhetsnivå 3. For at føderert identitetsforvaltning skal være et hensiktsmessig virkemiddel i kampen mot identitetstyveri er det helt essensielt at mekanismene som gir tilgang til personopplysinger er sterke.

Føderert identitetsforvaltning legger videre opp til mer spesialisering og samarbeid rundt identitetsforvaltning som i tur vil kunne øke kompetansenivået både med tanke på sikkerhet og personvern hos identitetsforvalterne. Det potensialet som ligger i arkitekturen aktualiserer også hensynet til personvern på en annen måte enn tidligere fordi arkitekturen i seg selv er tilrettelagt for det. Konkurranse i markedet om å ha det beste tilbudet til brukeren vil også i fremtiden kunne gjøre personvern og sikkerhetsspørsmål til salgsargumenter for identitetstilbyderen.

At den tekniske arkitekturen bak standarden for føderert identitetsforvaltning i seg selv er muliggjørende er imidlertid ingen garanti for bedre personvern og dermed redusert risiko for identitetstyveri. For brukerens del er man avhengige av at løsningene faktisk vektlegger pseudonymisering fremfor identifisering i de tilfeller hvor det er et alternativ. Hvorvidt dette skjer er noe vanskelig å vurdere ut fra løsningene jeg har sett på. MinID overfører fødselsnummer som en fast del av en påstand, men brukes foreløpig kun opp mot offentlige tjenester og gir derfor et tynt grunnlag for å foreta en vurdering. Ingen av tjenestene MinID gir tilgang på kan så vidt jeg vurderer sies å ikke ha behov for entydig identifisering ettersom det både i et sikkerhetsperspektiv og i et personvernperspektiv er viktig å ikke presentere informasjon om feil bruker.

FEIDE bruker mye tid på å fremheve attributtbasert autentisering og behovsprøvd utveksling av personopplysninger i sin løsning. Samtidig ser jeg av pålogging til BIBSYS gjennom FEIDE at opplysninger om fullt navn, fødselsnummer, e-post i tillegg til en rekke andre opplysninger[52] blir

52 https://idp.feide.no/simplesaml/module.php/feide/login.php?AuthState=_0b43210394e286248c9a4c88453d12ad9b9820add8%3Ahttps%3A%2F%2Fidp.feide.no%2Fsimplesaml%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Durn%253Amace%253Afeide.no%253Aservices%253Ano.bibsys.secure%253Aadgang#privacyframe

overført og delt i kommunikasjonen mellom FEIDE og BIBSYS. BIBSYS er en biblioteksressurs for studenter og ansatte som har FEIDE pålogging og gir brukere tilgang til å bestille bøker og publikasjoner fra en hel rekke forskjellige bibliotek landet over. Uten å gå inn i en diskusjon rundt behovet for hver enkelt opplysning synes det spesielt at BIBSYS har behov for alle disse. Etter min mening illustrerer dette et poeng i forhold til at muligheter og potensial ikke nødvendigvis medfører minimalitet i utveksling av personinformasjon. Dette er også et viktig poeng å ta med seg når føderert identitetsforvaltning og SAML etter hvert finner veien til det kommersielle markedet i Norge. Standarden slik jeg ser det er imidlertid et viktig steg mot sikrere elektronisk identitetsforvaltning, og vil uavhengig av hvordan andre personvernhensyn blir ivaretatt kunne representere en del av løsningen for å motvirke elektronisk identitetstyveri.

5.4 Autentisering ved bruk av biometri

5.4.1 Innledning

Biometri stammer fra det greske *bios* som betyr liv og *metri* som betyr måling, og betyr måling av biometriske mønster. Biologiske mønstre kan være knyttet til enten fysiologiske eller adferdsmessige trekk ved en person. Fysiologiske trekk er knyttet til det fysiske: fingeravtrykk, ansiktsform og lignende. Biometriske kjennetegn avgrenser seg dermed til det som er observerbart ved en person. (Liu 2007, side 4) Adferdsmessige trekk er knyttet til eksempelvis dynamikken i en signatur eller ganglaget til en person. Mennesker anvender biometri naturlig hver dag når vi gjenkjenner mennesker. Om biometri skal kunne ha en generell anvendelse som identifiserings- og autentiseringsmekanisme er man derimot avhengige av å benytte seg av elektroniske hjelpemidler som kan hjelpe oss å sammenlikne for eksempelvis fingeravtrykk og med stor grad av sikkerhet fastslå likhet eller ulikhet. Slike systemer kaller vi for biometriske systemer. De mest anvendte biometriske metodene i slike systemer inkluderer sammenlikning av

- fingeravtrykk,
- håndavtrykk,
- håndgeometri,
- signaturdynamikk,
- stemme,
- regnbuehinne (iris),

- netthinne (retina)
- kroppslukt,
- ganglag og
- ansikt.

Det som kjennetegner målbare biometriske mønstre er at de må være *universelle*, samtidig som de også må være *unike (uniqueness)*. Videre må mønstrene være *permanente (permanence)* over tid og de må være *kvantifiserbare (collectability)*, dvs. mulig å måle og registrere. I praksis har man også erfart at mønstrenes *prestasjon (performance)* i forhold til hvor nøyaktig de kan måles er viktig, noe som igjen vil kunne påvirke hvor lett det er å *omgå (circumvent)* systemet. Avslutningsvis er det en faktor at biometriske mønstre ikke kan benyttes i et biometrisk system dersom det ikke finnes *aksept (acceptability)* for bruken blant brukerne. (Jain, Ross & Prabhakar 2004, side 2)

Det har vært diskutert hvorvidt biometriske kjennetegn går inn under personopplysningslovens definisjon av personopplysning i § 2-1. I følge denne er en personopplysning *opplysinger og vurderinger som kan knyttes til en enkeltperson.* Det er umulig for den enkelte av oss å knytte et fingeravtrykk til et individ uten bruk av et biometrisk system. Det er imidlertid nok at identifisering *kan* skje, (Schartum & Bygrave 2004, side 114) noe som er tilfelle med biometriske data.

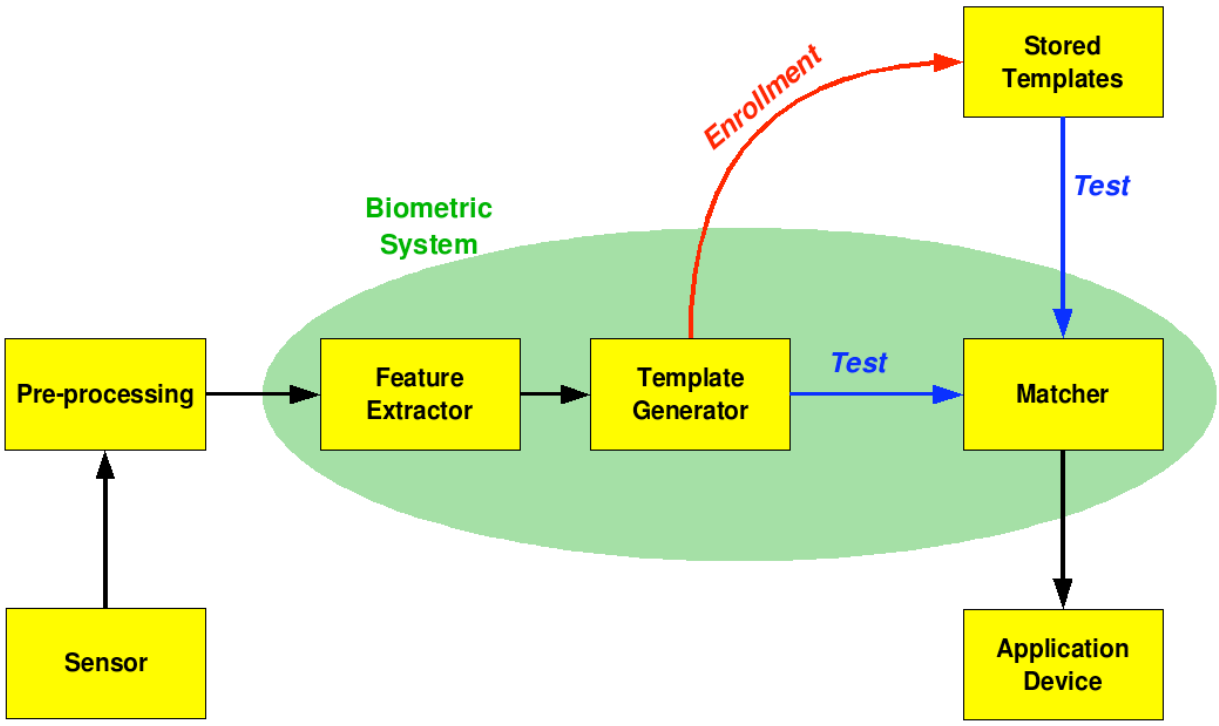
5.4.2 Bruksområder for biometriske system

Biometriske kjennetegn kan brukes i en rekke sammenhenger for å identifisere og autentisere. For privat bruk har det den siste tiden kommet flere datamaskiner og telefoner som bruker fingeravtrykk ved pålogging. Det finnes også system hvor biometriske data fungerer som tenningsnøkkel til en bil eller som nøkkel til et hus. Det finnes videre ”anonyme” løsninger hvor biometriske kjennetegn knyttes til en rettighet som for eksempel tilgang til et garderobeskap i en svømmehall. Slike løsninger vil kunne legges opp slik at fingeravtrykket slettes etter bruk. Bruk av biometriske kjennetegner er videre brukt som adgangskontroll til både fysiske områder og til informasjonssystemer, da gjerne i kombinasjon med et passord. Registreringsløsninger som for eksempel stemplingstjenester på arbeidsplasser finnes også med bruk av biometriske kjennetegn som erstatning for tradisjonelle identifikatorer og autentifikatorer. Ifølge Datatilsynet er dette løsninger som er relevante i forbindelse med bruk av biometriske kjennetegn. (Datatilsynet 2006, side 5-8)

Mest aktuelt i dagens samfunn er sammenlikning av fingeravtrykk som de seneste årene har fått en stadig større utbredelse. Flere saker avgjort av Personvernnemnda[53] har godkjent bruk av fingeravtrykksleser for sikker autentisering. I det følgende skal jeg se nærmere på hvordan et system for sammenlikning av fingeravtrykk kan fungere. Metoden vil i prinsippet kunne være den samme også for andre typer biometriske systemer.

5.4.3 Fingeravtrykk

Et system for sammenlikning av fingeravtrykk vil være et identitetsforvaltningssystem. Ved innrullering i et slik system må brukeren som oftest oppi separat *identifikator* og *autentifikator*.



Figur 46: Modell av biometriske system [54]

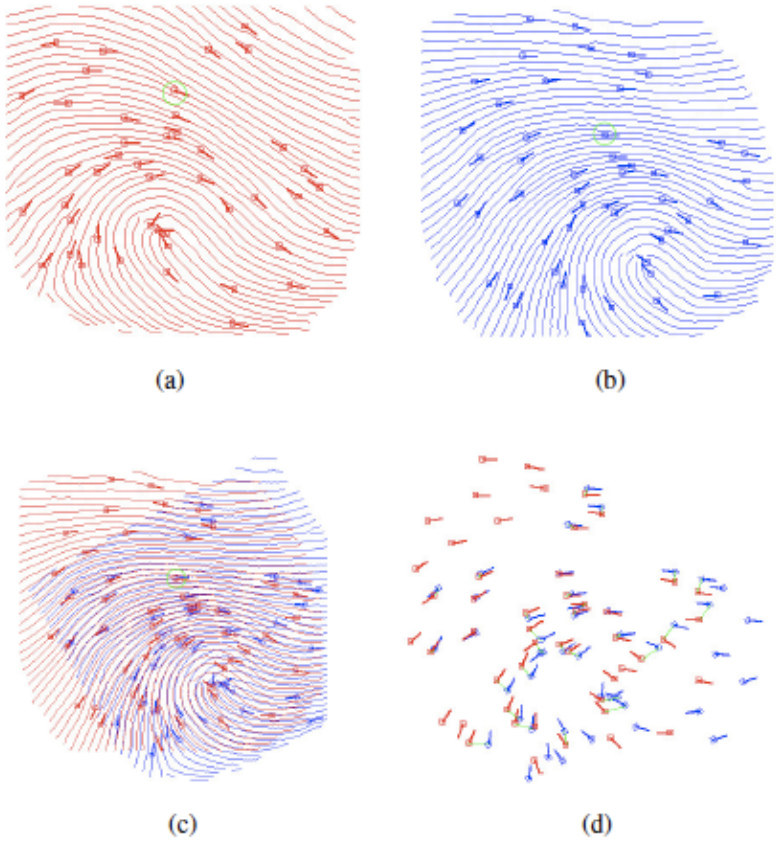
Identifikatoren er gjerne et passord eller en pinkode som kombineres med det biometriske kjennetegnet. Pinkoden er det som skiller brukeren fra alle andre brukere, mens det biometriske kjennetegnet er autentifikatoren som bekrefter at brukeren er den han utgir seg for å være. Ikke hele

[53] http://www.personvernnemnda.no/vedtak/index.htm Flere vedtak er å finne fra 2007 og 2006.

[54] http://en.wikipedia.org/wiki/Biometrics

Også gjengitt av Schartum og Bygrave (2008, side 16)

fingeravtrykket registreres, men et utsnitt som er nok til å gjenkjenne dette som unikt. Dette kalles for en *template*, og kan ikke fullt ut rekonstruere fingeravtrykket i sin helhet. Dette er i følge Datatilsynet (Datatilsynet 2006, side 4) mindre personvernkrenkende enn ved bruk av hele avtrykket fordi man reduserer mulighetene for senere misbruk. Ved senere innlogging vil brukeren identifisere seg med pinkode/passord og autentisere seg med fingeravtrykket. Figur 18 viser en slik prosess hvor man har fingeravtrykket brukeren avgir til leseren (a), templaten som er lagret i systemet (b) og matchingen (c og d). Her ser man hvilke punkter avleseren markerer og hvordan dette blir sammenliknet. I dette tilfellet var matchingsprosenten bare 37.



Figur 47: Fingeravtrykkmatching (Jain, Bolle & Pankanti 1999, side 29)

En annen måte å bruke et slikt system på er ved å kun identifisere ved bruk av fingeravtrykk. Et slikt system kan ha flere bruksmåter, spesielt i situasjoner hvor brukerens identitet ikke er vesentlig. SAS Braathens benytter en løsning hvor brukeren registrerer fingeravtrykket sitt ved innsjekking av bagasje. Utsnittet av dette lagres i en template men knyttes ikke til bookinginformasjon og benyttes

kun for å sjekke at den personen som sjekker inn bagasjen er den samme som faktisk går om bord i flyet. Templaten slettes sågar når reisen er gjennomført, eller i praksis innen 24 timer[55].

En metode for å gjøre biometri enda mer sikkert kalles for multimodal biometri. (Jain, Bolle & Pankanti 1999, side 34) Multimodal biometri kombinerer to eller flere biometriske kjennetegn, for eksempel fingeravtrykk og irisavlesning.

5.4.4 Rettslig adgang til bruk av biometriske system

Jeg skal ikke gå dypere inn i regelverket enn å se på vurderinger gjort av Datatilsynet og Personvernnemda med tanke på rettslig adgang til bruk av biometriske system.

Bruk av biometriske system for entydig identifisering og autentisering er omstridt, hovedsaklig på grunn av personopplysningsloven § 12 som regulerer entydige identifikasjonsmidler, og da i forhold til om biometriske kjennetegn er slike. Det synes å være enighet om at det er det og at § 12 skal anvendes, og dermed vil bruk av biometri være lovlig dersom det foreligger et saklig behov og metoden er nødvendig for å oppnå entydig identifisering.

Personopplysningsloven § 12 er i følge Datatilsynet utformet med henblikk på å hindre misbruk av fødselsnummer, men i forarbeidene nevnes biometri som eksempel på et entydig identifikasjonsmiddel[56]. Datatilsynet mener imidlertid at forarbeidene ikke tok høyde for de egenskapene biometri har i forhold til også å autentisere brukere. ”Fødselsnummer er uegnet som legitimasjon eller for å bekrefte identitet, mens en sammenligning av biometriske prøver nettopp er egnet for dette. Dette gjør at regelen er lite hensiktsmessig hva gjelder bruk av biometriske kjennetegn.” (Datatilsynet 2006, side 12) Tilsynet har derfor ytret ønske om endring av loven slik at man får en avklaring på hvordan man skal forholde seg til den økende pågangen rundt biometriske system. Forvaltningspraksis fra Personvernnemda har imidlertid vist en relativt positiv holdning til biometri og også Datatilsynet stiller seg positive til endringer i regelverket som åpner for mer bruk. (Datatilsynet 2006, side 12) Tendensene er altså stadig større rettslig aksept og dermed vil vi i samfunnet sannsynligvis se stadig flere autentiseringsløsninger som bygger på bruk av biometri.

[55] http://www.sas.no/no/Alt-om-reisen/Biometri/

[56] Se hvor Personvernnemda og Datatilsynet diskuterer denne og andre problemstillinger knyttet til biometri mer inngående. http://www.personvernnemnda.no/vedtak/2006_7.htm

5.4.5 Utfordringer knyttet til bruk av biometriske kjennetegn

Fordelene med biometriske mønstre er at de er uløselig knyttet til en persons fysiske karakteristika og dermed godt egnet til sikker identifisering og autentisering: man kan ikke miste, glemme eller få slike frastjålet. Dermed reduserer man sjansene for identitetsmisbruk På den andre siden vil konsekvensene sannsynligvis blir ekstra belastende nettopp fordi biometriske kjennetegn som metode er ansett for å være svært sikker og dermed i) vil kunne gi tilgang til mye informasjon og ii) gjøre det vanskelig å bli trodd dersom man hevder man er blitt utsatt for misbruk. Identitetstyveri hvor biometriske mønstre er inkludert vil dermed være en større utfordring å håndtere enn tradisjonelle karakteristika som brukernavn og passord. Farene med bruk av biometri finner vi både ved initiell innrullering og ved senere autentisering og kan forekomme som resultat av

- dårlig teknologi eller
- menneskelig svikt.

Som illustrert vil det i et biometrisk system lagres en template som er et utsnitt av for eksempel et fingeravtrykk. Kvaliteten på systemet avhenger av hvor detaljert denne templaten er, altså hvor mange punkter i fingeravtrykket systemet registrerer og senere sammenlikner med. Et dårlig system vil kunne godkjenne fingeravtrykk som likner på eller er et påmontert avtrykk. Bruk av multimodale biometriske systemer vil imidlertid vesentlig redusere risikoen for en slik svikt. Menneskelig svikt kan oppstå i innrulleringen dersom en person blir registrert inn med en annen identitet enn sin egen. Ettersom biometriske system er løsninger som representerer sikker identifisering vil slike feil kunne medføre ekstra store konsekvenser. Dette fordi man potensielt vil kunne få tilgang til mye ressurser samtidig som det vil kunne være vanskeligere å bevise sin uskyld i og med at teknologien er svært sikkert og nyter stor tillit som sikker løsning. Troen på teknologiens ufeilbarlighet kan dermed bli en fare i seg selv. Spørsmålet er om autentiseringsmetoder med så sterk grad av tilknytning til et individ og som i utgangspunktet har så stor tillitt kan tillate seg feilmarginer i det hele tatt.

5.4.6 Samlet vurdering

Mange betrakter biometri som en rask, effektiv og sikker løsning for å bekrefte at en person er den hun eller han utgir seg ut for å være. Man trenger ikke ha med seg noe som kan mistes, stjeles eller huske noe som kan glemmes fordi biometrien er uløselig knyttet til et individ. Bruk av biometri kan være et godt bidrag til å utvikle sikre løsninger mot autentisering av feil person og dermed motvirke identitetstyveri. Forutsetningen for at biometri er et godt tiltak er imidlertid at løsningene som

benyttes er sikre mot misbruk. Dersom dette ikke er tilfelle vil de samme grunnene som taler til fordel for biometri være det som også taler mot det. Dersom man tar utgangspunkt i at løsningene som eventuelt blir rullet ut er sikre nok er spørsmålet i hvilke tilfeller biometri er egnet som autentiseringsmekanisme. Først og fremst vil dette gjelde i tilfeller hvor det er behov for autentisering av *individ.* I kombinasjon med noe personen *har* eller *vet* vil biometri kunne gi svært god sikkerhet og i vesentlig grad være med å redusere risikoen for identitetstyveri. Man kan imidlertid også se for seg løsninger som benytter biometri for å autentisere en tilbakevendende bruker uten at denne blir identifisert. Faren med dette i et identitetstyveriperspektiv er at dette fører til økt eksponering og dermed også økte muligheter for identitetstyveri. Hvor store konsekvenser slikt vil føre til eller om det vil få konsekvenser i det hele tatt er imidlertid umulig å si noe om da fordi dette avhenger av flere faktorer, blant annet hva slags utbredelse teknologien vil få i samfunnet og ikke minst hvor stor forskjell det vil være på teknologiene som brukes til ulike formål. En fingeravtrykksleser brukt i et garderobeskap kan eksempelvis kunne tenkes å være helt harmløst dersom den lagrede templaten er av vesentlig dårligere kvalitet enn systemer som gir tilgang til sensitive personopplysninger. Utstrakt bruk av biometri i slike tilfeller vil mest sannsynlig ikke bli tatt i storskala bruk i offentligheten. Dette fordi dagens lovgivning gjennom personopplysningsloven § 12 setter begrensninger for når biometri kan tas i bruk, jf. avsnitt 5.4.4. Et forbehold må likevel tas i denne sammenheng da Personvernnemda i sak PVN-2006-07[57] skriver at en template i seg selv ikke er et entydig identifikasjonsmiddel. Et garderobeskap som ikke lagrer noe annet enn en template vil dermed kunne slippe den strenge vurderingen det legges opp til i § 12 og i teorien vil samtykke etter § 8 være lovlig behandlingsgrunnlag. Jeg skal ikke gå nærmere inn i denne diskusjonen, men kan påpeke at det pågår et arbeid med å endre loven i retning av å være mindre restriktive[58]. Jeg vil imidlertid konkludere med at det fra et identitetstyveriperspektiv er hensiktsmessig å ta i bruk biometri.

5.5 Organisatoriske og pedagogiske tiltak

Tekniske løsninger for sikring av konfidensialitet, integritet og sikker autentisering må følges opp av andre tekniske og organisatoriske tiltak samt. Slike tiltak retter seg mot intern sikring av elektroniske informasjonsressurser og mot rutiner for håndtering av informasjon i fysiske medier. Kapittel 4.4 og 4.6 illustrerte og identifiserte ikke-tekniske trusler mot personopplysningers konfidensialitet og integritet. Dette avsnittet tar utgangspunkt i funnene derfra. Juridiske tiltak er for

[57] http://www.personvernnemnda.no/vedtak/2006_7.htm

[58] Se Schartum og Bygrave 2008.

øvrig også viktig for å underbygge andre tiltak. Jeg anser imidlertid det rettslige aspektet ved gjennomgangen av ny bestemmelse i § 202 i kapittel 2 og gjeldende rett i kapittel 3.

5.5.1 Organisatoriske tiltak

Tiltakene som er diskutert frem til nå i dette kapittelet har omhandlet tiltak som går på utforming av identitetsforvaltningssystemer og teknologiske sikringsmekanismer. Et annet aspekt ved sikkerheten handler imidlertid om sikkerhetsrutiner, retningslinjer for bruk og ikke minst hvilken informasjon den enkelte bruker skal ha tilgang på i systemet. Slike tiltak omtales som organisatoriske tiltak, selv om de også kan være av teknisk art. (Teknologirådet 2005, side 92)

En sentral problemstilling er knyttet til problemer med egne ansatte som misbruker arbeidsgivers informasjonsressurser. Som illustrert i avsnitt 4.4 er dette utelukkende den største kilden for sikkerhetsbrudd hos tjenesteleverandører, noe som også hevdes av Teknologirådet i sin rapport om elektroniske spor og personvern- (Teknologirådet 2005, side 92) Tiltak som kan motvirke slike hendelser handler om mer finkornet *tilgangsstyring* for å sikre tilgang etter behov. Dette sikrer at brukere med ulikt behov får tilgang til ulike deler av for eksempel en database med personopplysinger. Enterprise Privacy Authorization Language (EPAL) er et eksempel på en teknisk løsning for finkornet tildeling av brukerrettigheter.

EPAL definerer et sett av opplysningskategorier, brukerkategorier, behandlingsformål, behandlingskategorier, forpliktelser og betingelser. Ut i fra disse lages regler som på bakgrunn av dato, bruker og behandlingsformål enten tillater eller nekter en konkret behandling av personopplysninger. Kategoriseringen av ulike dataelementer fastsettes individuelt på bakgrunn av selskapets retningslinjer for vern av personopplysninger, samt den lovgivning man er underlagt ved behandling av slike opplysninger. Ved bruk av slik programvare kan den enkelte ansattes tilgang vesentlig reduseres og dermed også eksponeringen av personopplysninger. Jeg skal ikke gå nærmere inn på EPAL men vil konkludere med at prinsippene i teknologien vil være et vesentlig bidrag i retning av mindre tilgjengeliggjøring av personopplysninger og dermed også mindre risiko for identitetstyveri[59].

Det finnes betydelige utfordringer når det gjelder måten sensitiv eller beskyttelsesverdig informasjon utveksles fysisk mellom aktører i samfunnet. I svært mange tilfeller distribueres slike opplysninger via vanlig postgang til postkasser uten sikring. Dette kan være selvangivelser, bank-

[59] For mer om EPAL se teknologirådet 2005 side 95.

og kredittkort og pinkoder til MinID for å nevne noen få eksempler. Tre mulige tiltak kan skisseres i slike tilfeller:

- ikke bruke postgang
- sende rekommandert eller
- bruk av hengelås på kostkasser

Man kan se for seg løsninger hvor sensitive dokument fra det offentlige i større grad blir tilgjengeliggjort i MinSide slik at man dermed slipper risikoelementene knyttet til både forsending og oppbevaring hos posten og i postkasse. Det er imidlertid et viktig prinsipp i forvaltningen at det skal finnes likeverdige alternativer til elektronisk post eller tilgjengeliggjøring. Alternativt kan sensitiv informasjon gjøres tilgjengelig ved personlig oppmøte eller sendes som rekommandert post. Begge disse alternativene har imidlertid sine begrensninger. Personlig oppmøte for å hente selvangivelser vil potensielt kunne medføre et logistikkproblem. Det samme gjelder for rekommanderte sendinger som krever personlig oppmøte og legitimering ved postkontor. Rekommandert post hefter også ved seg et økonomisk aspekt da dette er en betydelig dyrere ordning enn ved vanlig a-post[60]. Bruk av hengelås på postkasser er noe som i lengre tid er blitt forfektet av Datatilsynet. (Datatilsynet 2009, side 16) Dette er et forholdsvis enkelt tiltak som kan utgjøre en stor forskjell. Alle disse tiltakene burde kunne gjennomføres hver for seg og i ulike situasjoner med sikte på å redusere tilgjengeligheten for personopplysninger i fysiske medier.

5.5.2 Pedagogiske tiltak

Et av hovedfunnene i kapittel 4 var at brukerne selv i veldig stor grad er utsatt for trusler og hendelser som kan føre til identitetstyveri gjennom dårlig sikring av både elektroniske og fysiske ressurser. Selv om internett har vært en viktig del av hverdagslivet for mange siden midten av 90-tallet eller nærmere årtusenskiftet er det likevel nærliggende å tro at kompetansenivået hos mange likevel ikke er tilstrekkelig, noe tallene i kapittel 4 i hvert fall til dels bekrefter. Tiltak for å motvirke dette kan komme i form av inforasjonskampanjer for å bevisstgjøre den enkelte bruker om sitt selvstendige ansvar for å sikre egne elektroniske og fysiske ressurser mot uautorisert innsyn.

[60] http://www.posten.no/Produkter+og+tjenester/Brev+og+frimerker/2614.cms

5.6 Konklusjon og oppsummering

Identitetstyveri kan motvirkes på flere ulike måter: personvernøkende teknologi kan sikre anonymitet, føderert identitetsforvaltning kan balansere samfunnets behov for identifisering med individets krav på anonymitet mens biometriske system for autentisering vil kunne skape nødvendig trygghet for begge parter i elektronisk kommunikasjon.

Jeg vil konkludere med at alle løsningene diskutert i dette kapittelet har en rolle å spille i bekjempelsen av identitetstyveri, men i ulike situasjoner. Anonymitet bør bestrebes i tilfeller hvor det ikke er nødvendig med identifisering, og bør stå som en målsetning og inspirere til utvikling av løsninger som lagrer og behandler et minimum av personopplysninger. For nettopp fravær av opplysninger som kan misbrukes er det mest virkningsfulle tiltaket man kan iverksette mot identitetstyveri. Sterk identifisering og autentisering og bruk av biometri er derimot både ønskelig og hensiktsmessig for løsninger som inneholder stort omfang av personopplysninger. Problemene oppstår imidlertid i situasjoner hvor dette ikke er like klart. Datatilsynets bekymring for overeksponering av identitetsdata, jf. avsnitt 5.2.1, siktet til slike situasjoner og faren for å kreve for sterk identifisering. Nøkkelen slik jeg ser det er å innta en restriktiv holdning til når det er nødvendig å identifisere.

Sterke mekanismer for identifisering og autentisering av brukere har den fordelen at de er vanskelige å omgå og dermed gir trygghet mot identitetstyveri. Spesielt gjelder dette biometri som er et entydig identifikasjonsmiddel og uløselig knyttet til hver enkelt menneske. Samtidig vil slike løsninger også kunne representere en trussel mot både brukere og tjenesteleverandører. Dette fordi slike løsninger generelt vil nyte stor tillitt og dermed kunne gi tilgang til mye ressurser og tjenester som i tur vil medføre stor skade ved misbruk. Anonym kommunikasjon vil imidlertid helt umuliggjøre identitetstyveri fordi det å være anonym innebærer et fravær av identifiserende opplysinger som kan misbrukes. Fullstendig anonym opptreden i elektroniske medier er imidlertid en utopi da samfunnet i mange tilfeller har et reelt behov for å vite hvem man kommuniserer med. Jeg vil imidlertid argumentere for at det er mulig å kombinere sterk identifisering og autentisering med anonymitet. Løsninger for føderert identitetsforvaltning muliggjør dette ved at en bruker kan identifisere seg hos en tiltrodd identitetsforvalter mens senere kommunikasjon med tjenesteleverandører kan gjøres under pseudonym eller ved attributtbasert autentisering. Samfunnet vil på denne måten få tilfredsstilt sitt behov for identifisering ved at brukerens identitet ved behov

kan utleveres[61], samtidig som brukeren vil være anonym overfor den andre part. At den tekniske arkitekturen bak standarden for føderert identitetsforvaltning i seg selv er muliggjørende er imidlertid ingen garanti for bedre personvern, og dermed redusert risiko for identitetstyveri. For brukerens del er man avhengige av at løsningene faktisk vektlegger pseudonymisering fremfor identifisering i de tilfeller hvor dette er et alternativ. Standarden slik jeg ser det er imidlertid et viktig steg mot sikrere elektronisk identitetsforvaltning, og vil uavhengig av hvordan andre personvernhensyn blir ivaretatt kunne representere en del av løsningen for å motvirke elektronisk identitetstyveri.

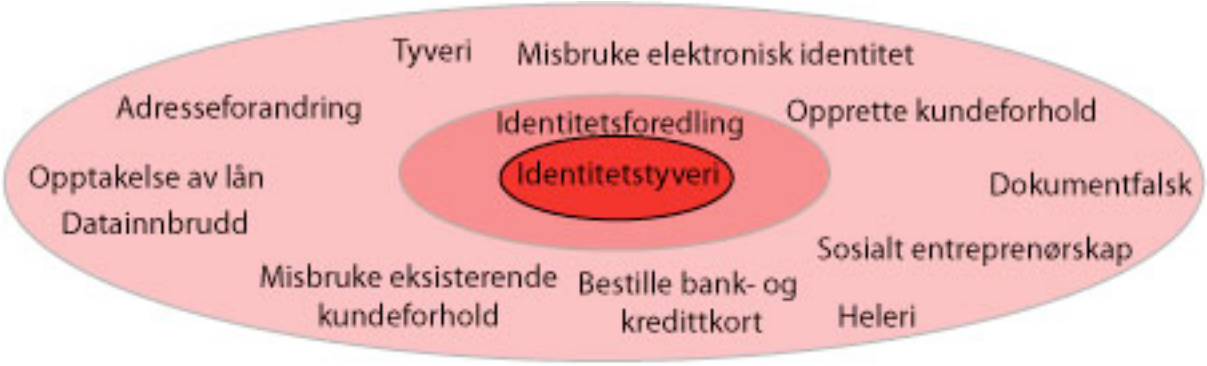
Faser	***Trusler***	***Tiltak***	***Vurdering***
Tilegnelse	Konfidensialitets og integritetsbrudd	Fravær av personopplysninger, personvernøkende identitetsforvaltning, lås på postkasser, finkornet tildeling av brukerrettigheter, pedagogiske tiltak.	Hvor bra tiltaket er avhenger av implementeringen
Videreforedling	Konfidensialitet, integritet og autentisering	Bruk av biometri for autentisering av brukere	Er hensiktsmessig i visse situasjoner men har svakheter.
Svindel	Svak autentisering	Bruk av biometri for autentisering av brukere	Er hensiktsmessig i visse situasjoner men har svakheter.

Tabell 3: Tiltaksmodell

[61] Eksempelvis gjennom rettslig kjennelse om utlevering slik vi i dag kjenner det fra saker om utlevering av IP-adresser.

Avslutning

Ved å kalle noe et tyveri insinuerer man at noe blir tatt fra noen. Kritikken mot begrepet har vært rettet mot nettopp det poenget at en identitet ikke kan stjeles på en slik måte. En identitet kan kopieres og misbrukes, men identitetsholderen mister ikke sin identitet selv om noen andre også utgir seg for å være denne. Dette er imidlertid en sannhet med modifikasjoner. Elektroniske identiteter er fullt mulig å stjele i den forstand at identitetsholderen kan miste tilgangen til brukerkontoer. Det finnes også tilfeller hvor personer vil kunne oppleve at identiteten deres blir sperret gjennom kredittnekt, noe som kan gi en følelse av å ha blitt frastjålet sin identitet. Etter min mening må begrepets vage innhold ta mye av skylden for kritikken som rettes mot det. Det er vanskelig å akseptere en såpass sterk karakteristikk når begrepet favner så bredt som det synes å gjøre i litteraturen. Basert på gjennomgangen og analysen foretatt i denne oppgaven har jeg derfor kommet frem til at det er hensiktsmessig å snevre inn forståelsen av hva et identitetstyveri er. Jeg ønsker derfor å skille identitetstyveri fra det jeg vil kalle *annen identitetsrelatert kriminalitet*. Grunnen for å gjøre en slik sondring er for det første å forbeholde begrepet identitetstyveri om et alvorlig brudd på den *enkeltes integritet*. Dette medfører å skille mellom enkle former for kortmisbruk, økonomisk svindel og bedrageri i forhold til identitetstyveri av mer systematisk karakter. Videre er noe av grunnen at mange av elementene i et identitetstyveri allerede har andre betegnelser, i samfunnet generelt og lovverket spesielt som gjennomgangen i kapittel 3 viser. Det virker lite hensiktsmessig å bruke ulike betegnelser på en og samme ting. Det som kjennetegner et identitetstyveri er at det tar opp i seg mange ulike elementer og handlinger, som illustrert i figur 24 under.



Figur 48: Identitetsrelatert kriminalitet

Etter min mening er ikke enkelttilfeller av identitetsmisbruk som identitetstyveri å regne, dette er heller et element i et identitetstyveri. Et identitetstyveri kjennetegnes derimot gjennom i større grad å være systematisert gjennom videreforedling av identiteter, slik prosessbeskrivelsen i kapittel 4 viste. Hvor mange element et identitetstyveri består av må bero på en vurdering hvor totalen av den tilegnede informasjonen må være avgjørende. På bakgrunn av dette har jeg kommet frem til at identitetstyveri kan defineres på følgende måte:

"Systematisk identitetsforedling gjennom tilegnelse, besittelse, overføring, reproduksjon eller annen manipulering av en annens personlige informasjon med det formål å begå gjentatt identitetssvindel for selv å oppnå fordeler eller å utsette andre for ulemper vil være å regne som identitetstyveri."

I motsetning til de mer vidtgående definisjonene jeg gjennomgikk i kapittel 2 snevrer denne definisjonen inn forståelsen av begrepet for å avgrense fra tilfeller som synes urimelig å omfatte. Kravet om *identitetsforedling* medfører at definisjonen legger til grunn at et identitetstyveri er et resultat av gjentatt og systematisk personprofilering. Videre setter definisjonen opp et krav om at hensikten er *"systematisert og gjentatt identitetssvindel"*. Dette innebærer at et identitetstyveri har forekommet dersom man gjentatte ganger blir utsatt for misbruk av egen identitet. På bakgrunn av det arbeidet jeg har gjort i denne oppgaven innebærer dermed et identitetstyveri å miste kontrollen over bruken av egen identitet.

Kildeliste

Bøker:

Boe, Erik. 2005. *Grunnleggende juridisk metode - En introduksjon til rett og rettstenkning*. Oslo: Universitetsforlaget.

Bratholm, Anders og Magnus Matningsdal. 1995 *Straffeloven med kommentarer. Anden del. Forbrydelser.* Oslo: Universitetsforlaget.

Hellevik, Ottar. 7. utgave 2. opplag 2003. *Forskningsmetode i sosiologi og statsvitenskap*. Oslo: Universitetsforlaget.

Jansen, Arild og Dag Wiese Schartum. 2005. *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT.* Oslo: Fagbokforlaget.

Lessig, Lawrence. 2006. *Code and other laws of Cyberspace, version 2.0*. New York: Basicbooks

Linninger, Rachel & Russel Dean Vines. 2005. *Phishing. Cutting the Identity Theft Line*. Indianapolis: Wiley Publishing.

Schartum, Dag Wiese og Lee Bygrave. 2004. *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.* Oslo: Fagbokforlaget.

Språkrådet. 2008. *Termlosen. Kort innføring i begrepsanalyse og terminologiarbeid*. Oslo: www.kursiv.no

Artikler:

Aarseth, Espen. 2008. Virtuell virkelighet og retorikk - en kritikk av virtualitetsbegrepet.
Tilgjengelig: http://www.hf.uib.no/hi/espen/VV-retorikk.html
Sist besøkt 19 februar 2009

Burkert, Herbert, Philip Agre og Marc Rotenberg (red). 1997. *Privacy-enhancing technologies: typology, critique, vision*, i Technology and privacy: the new landscape, Cambridge Massachusetts, 1997.
Tilgjengelig: http://wiki.urban.cens.ucla.edu/images/7/75/Burkert_-_Privacy-enhancing_technologies_-_shrunk.pdf
Sist besøkt 27 april 2009

Bygrave, Lee. 1998. *Data Protection Pursuant to Privacy in Human Rights Treaties*, i International Journal of Law and Information Technology, 1998 volume 6, Oxford University Press.
Tilgjengelig: http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf
Sist besøkt 27 april 2009

Reidenberg, Joel. 1998. *Lex Informatica: The formulation of information policy rules through technology.* Texas Law Review, volume 76 number 3.

Symantec. 2006. *"Pharming". Når phishing angrep utvikler seg og gjør det umulig å oppdage.*
Tilgjengelig: http://www.symantec.com/no/no/norton/library/article.jsp?aid=article1_08_06
Sist besøkt 19 februar 2009

Publikasjoner:

Anti Phishing Working Group (APWG). 2008. *Phishing Activity trends Report Q1 2008.*
Tilgjengelig: http://www.apwg.org/reports/apwg_report_Q1_2008.pdf
Sist besøkt 19 februar 2009

CIPPIC. Mars 2007a. *Identity Theft: Introduction and Background, CIPPIC Working Paper No.1 (ID Theft Series)*. Ottawa.
Tilgjengelig: http://www.cippic.ca/documents/bulletins/Introduction.pdf
Sist besøkt 27 april 2009

CIPPIC. Mars 2007b. *Techniques of Identity Theft, CIPPIC Working Paper No.2 (ID Theft Series)*. Ottawa.
Tilgjengelig: http://www.cippic.ca/documents/bulletins/Techniques.pdf
Sist besøkt 27 april 2009

CIPPIC. April 2007c. *Caselaw on Identity Theft, CIPPIC Working Paper No.4 (ID Theft Series)*. Ottawa.
Tilgjengelig: http://www.cippic.ca/documents/bulletins/CaseLaw_April%2011%2C%202007.pdf
Sist besøkt 27 april 2009

CIPPIC. Mai 2007d. *Policy Approaches to Identity Theft, CIPPIC Working Paper No.6 (ID Theft Series)*. Ottawa.
Tilgjengelig: http://www.cippic.ca/documents/bulletins/Policies.pdf
Sist besøkt 27 april 2009

CIPPIC. April 2007e. *Identity Theft: A Bibliography, CIPPIC Working Paper No.7 (ID Theft Series)*. Ottawa.
Tilgjengelig på: http://www.cippic.ca/documents/bulletins/Bibliography.pdf
Sist besøkt 27 april 2009

Finansnæringens Hovedorganisasjon (FNH). 2008. *Felles utfordringer knyttet til identitetsmisbruk*.
Tilgjengelig: http://www.fnh.no/ID-Rapport,_9.oktober_2008_DjppR.pdf.file
Sist besøkt 27 april 2009

Frei, Stefan, Thomas Duebendorfer, Gunter Ollman & Martin May. 2008. *Understanding the Web browser threat: Examination of vulnerable Web browser population and the "insecurity iceberg"*. Zürich
Tilgjengelig på: http://www.techzoom.net/papers/browser_insecurity_iceberg_2008.pdf
Sist besøkt 19 februar 2009

Federal Trade Commission. 2007. *Talking about identitytheft: A how-to guide.*
Tilgjengelig: http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html#Howto
Sist besøkt 19 februar 2009

Jain, Anil, Arun Ross, Salil Prabhakar. 2004. *An introduction to biometric recognition.*
Tilgjengelig på:
http://www2.citer.wvu.edu/members/publications/files/RossBioIntro_CSVT2004.pdf
Sist besøkt 10 april 2009

Jain, Anil, Ruud Bolle, Sharath Pankanti. 1999. *Introduction to biometrics*, i BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, Michigan.
Tilgjengelig på: http://www.cse.msu.edu/~cse891/Sect601/textbook/1.pdf
Sist besøkt 10 april 2009

U.S Departement of Justice. 1998. *The Identity Theft and Assumption Deterrence Act of 1998*.
Tilgjengelig: http://www.ftc.gov/os/statutes/itada/itadact.htm
Sist besøkt 27 april 2009

Javelin Strategy & Research. 2006. *Identity Fraud Survey Report*. California.
Tilgjengelig: http://www.javelinstrategy.com/uploads/2006IDFBrochure.pdf
Sist besøkt: 25 november 2008.

Javelin Strategy & Research. 2008. *Identity Fraud Surveuy Report*. California.

OASIS. 2005. *SAML V2.0 Executive Overview. Committee Draft 01*.
Tilgjengelig: http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf
Sist besøkt 27 april 2009

OASIS. 2005b. *SAML V2.0 Executive Overview. Working draft 08.*
Tilgjengelig på: http://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf
Sist besøkt 26 mai 2009.

OASIS. 2008. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*.
Tilgengelig på: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf
Sist besøkt 26 mai 2009

Olsen, Thomas & Tobias Mahler. 2005. *Privacy - Identity Management. Data protection Issues in relation to Networked Organisations Utilizing Identity Management Systems*. Oslo

Tilgjengelig: http://193.72.209.176/Projects/P1084/D11%20Report%20on%20Privacy%20-%20Identity%20Management%20-%20site.pdf
Sist besøkt 27 april 2009

Pfitzmann, Andreas og Marit Hansen. 2005. *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*. Dresden.
Tilgjengelig på: http://www.freehaven.net/anonbib/cache/terminology.pdf
Sist besøkt 26 mai 2009.

Sproule, Susan & Norm Archer. 2007. *Defining Identity Theft*. wcmeb,pp.20, Eighth World Congress on the Management of eBusiness (WCMeB 2007).

The Presidents Identity Theft Task Force. 2007. *Combating identity theft. A strategic plan.*
Tilgjengelig: http://www.identitytheft.gov/reports/StrategicPlan.pdf
Sist besøkt 19 februar 2009

Dokumenter fra det offentlige:

Datatilsynet. 2006. *Notat fra Datatilsynet – forslag til revisjon av personopplysningslovens § 12 og ny bestemmelse om bruk av biometriske data*.
Tilgjengelig på:
http://www.datatilsynet.no/upload/Dokumenter/saker/2006/Revisjon_12_biometri.pdf
Sist besøkt 26 mai 2009.

Datatilsynet. 2009. *Identitetstyveri*. Oslo
Tilgjengelig:
http://www.datatilsynet.no/upload/Dokumenter/utredninger%20av%20Datatilsynet/Utredning%20om%20ID-tyveri.pdf
Sist besøkt 26 mai 2009.

Datatilsynet. 2007. Høring – Forslag til strategi for bruk av eID og e-signatur i offentlig sektor. Oslo. Tilgjengelig på:
http://www.datatilsynet.no/upload/07-00401-2.pdf
Sist besøkt 26 mai 2009.

FEIDE systemarkitektur versjon 2.0.
Tilgjengelig: http://docs.feide.no/guide-0004
Sist besøkt 27 april 2009

Fornyings- og Administrasjonsdepartementet. 2007. *Høringsversjon. Strategi for eID og eSignatur i offentlig sektor. Versjon 1.0*. Oslo

Justis- og Politidepartementet. 2007. *Nasjonalt ID-kort. Sluttrapport februar 2007*.
Moderniseringsdepartementet. 2005a. *Kravspesifikasjon for PKI i offentlig sektor versjon 1.02*.
Tilgjengelig på: http://www.regjeringen.no/upload/kilde/mod/rap/2004/0002/ddd/pdfv/234033-kravspek_pki_v102.pdf
Sist besøkt 26 mai 2009.

Moderniseringsdepartementet. 2005b. *Konsept for det virtuelle servicekontoret MinSide versjon 2.0*.
Tilgjengelig på:
http://www.hoykom.no/hoykom/HOYKOM_Prosjekter_ny.nsf/a1b9d00d779649e9c1256d7b0033f036/18976b3f2ccd7a26c1256fe7003fe13b/$FILE/Konsept%20MinSide%20040405.pdf
Sist besøkt 26 mai 2009.

NOU 1997: 19. *Et bedre personvern. Forslag til lov om behandling av personopplysninger*. Oslo

NOU 2001: 10. *Uten penn og blekk*.

NOU 2007: 2. *Lovtiltak mot datakriminalitet, delutredning II*. Oslo

NOU 2009: 1. *Individ og integritet. Personvern i det digitale samfunnet*. Oslo

Ot.prp. nr. 90 2003-2004. *Om lov om straff (Straffeloven)*. Oslo

Ot.prp. nr. 22 2008-2009. *Om lov om endringer i straffeloven 20 mai 2005 nr. 28. (Siste delproposisjon – sluttføring av spesiell del og tilpasning av annen lovgivning)*.

Schartum, Dag Wiese og Lee Bygrave. 2008. *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12*.
Tilgjengelig på:
http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/rapporter/2008/utredning-om-fodselsnummer-fingeravtrykk.html?id=534749&epslanguage=NO
Sist lest 17 desember 2008

SIFO. 2007. *Forbrukernes stilling i informasjonssamfunnet*.
Tilgjengelig på: http://www.sifo.no/files/file72368_bld-pres041207.pdf
Sist besøkt 26 mai 2009.

Software Innovation. 2006. *Implementation guide for federation. 0.7*.
Tilgjengelig på: http://www.difi.no/Implementation_guide_for_Minid_021106_DdYDf.pdf.file
Sist besøkt 26 mai 2009.

St.mld. nr.27 2006-2007. *Eit informasjonssamfunn for alle*. Oslo

Teknologirådet. 2005. *Elektroniske spor og personvern*. Oslo

Presentasjoner:

Direktoratet for Forvaltning og IKT. 2008. Planer for etablering av Samtrafikknavet. Oslo
Tilgjenglig: http://www.nokios.no/2008/_media/s2_c3_t_alvik.pdf?id=presentasjoner&cache=cache
Sist besøkt 23 februar 2008

Ellertsen, Kim. 2008. Mørketallsundersøkelsen 2008. Foredrag på Sikkerhetskonferansen 2008.

Lawson, Philippa. 2008. *Identity Theft: The Canadian Experience*.
Tilgjengelig: http://securityvalley.no/images/Documents/sikkerinfo2008/id-theft-canada-lawson.pdf
Sist besøkt 23 september 2008

Liu, Yue. Mars 2007. *Introduction to biometrics from å legal perspective*. Forelesning ved UiO Jur5630 våren 2008. Tilgjengelig på:
http://www.uio.no/studier/emner/jus/jus/JUR5630/v08/undervisningsmateriale/Introduction_to_biometrics_from_a_legal_perspective-1.ppt

Sist besøkt 26 mai 2009.

Nordseth, Gunnar. 2004. *Offentlig identitet og private personalia.*
Tilgjengelig:
http://eforum.custompublish.com/getfile.php/122549.367/Offentlig+identitet+og+private+personalia.pdf
Sist besøkt 27 april 2009

Vedlegg 1: Kvantitativ undersøkelse av nettartikler

For å danne meg et bilde av hvordan norske medier omtaler identitetstyveri tok jeg for meg nettavisene til Dagbladet, VG, Nettavisen, Aftenposten og Nordlys og foretok søk deres arkiver på ordet "identitetstyveri". Treffene valgte jeg å sortere etter relevans og plukket ut maks 10 saker per avis som jeg gikk gjennom og kategoriserte. Artiklene ble valgt tilfeldig, men ut fra noen kriterium. Jeg skulle:

- unngå artikler om samme sak i forskjellige aviser
- finne flest mulig artikler om norske forhold
- identitetstyveri måtte være en fremtredende del av artikkelen

Totalt fikk jeg 173 treff i de fem overnevnte avisene, og totalt plukket jeg ut 44 saker jeg gikk gjennom. Opprinnelig var tanken å gå gjennom 10 saker fra hver nettavis, jeg fant derimot bare 4 relevante saker hos avisen Nordlys. Av de 173 treffene måtte en god del kasseres fordi de ikke passet til de overnevnte kriteriene. Mange omtalte saker var fra USA spesielt , og var gjerne hentet fra internasjonale pressebyrå. Jeg var i min undersøkelse mer interessert i hvordan norske medier selv brukte begrepet. Mange saker var også gjengitt av flere aviser, og da flere ganger med bare marginale forskjeller i teksten. Jeg plukket i så fall ut bare en av disse. I mange av artiklene var identitetstyveri bare nevnt så vidt. Dette kunne gjerne være mer generelle artikler omkring sikkerhetsspørsmål hvor identitetstyveri kunne nevnes som en mulig konsekvens. Jeg prøvde å unngå de mest generelle artiklene da jeg anså disse som ikke representative for det jeg undersøkte. Søket hadde ikke noen begrensning i tid, og treffene jeg fikk var fra begynnelsen av 2000-tallet og frem til 2009.

Det overordnede spørsmålet jeg ønsket å få svar på var: hvordan bruker mediene begrepet identitetstyveri? For å svare på dette kategoriserte jeg først artiklene basert på om de omtalte identitetstyveri i forhold til

- uberettiget tilegnelse av personinformasjon,
- misbruk av personinformasjon
- eller begge deler.

Jeg gikk deretter videre med å ta for meg hva slags misbruk som ble satt i sammenheng med identitetstyveri. Kategoriene jeg brukte i denne sammenhengen ble hentet direkte fra artiklene, det var med andre ord ikke noe som ble satt opp på forhånd og som artiklene etterpå ble puttet inn i. Dette var

- Kredittsvindel
- Mobilssvindel
- Dokumentfalsk
- Misbruk av navn
- Misbruk av personnummer
- Adresseforandring posten
- Adresseforandring folkeregisteret
- Misbruk av identitetsbevis

På et punkt slo jeg sammen flere kategorier, og det var det som gikk på kredittsvindel. Jeg fant det hensiktsmessig å slå sammen misbruk av bankkort, kredittkort samt opptakelse av lån i andres navn til en samlet kategori som var misbruk av økonomisk art. Misbruk av identitetsbevis er brukt i saker av ikke-økonomisk karakter, dvs. misbruk av bankkort for uttak i minibank er ikke tatt med i denne kategorien. Fremvisning av en annens bankkort i skranken i banken ville derimot vært misbruk av identitetsbevis. Slik det er gjort i denne undersøkelsen vil kategorien misbruk av navn innebære misbruk av navn uten bruk av identifikasjonsbevis. Som eksempel kan nevnes forbrukerforskeren Runar Døving som ble omtalt som identitetstyv for å ha misbrukt navnet til reklamemannen Kjetil Try i en kronikk i Dagbladet. Om det hadde brukt et identitetsbevis for å understøtte påstanden ville det blitt karakterisert som misbruk av identitetsbevis.

Artiklene som er brukt er gjengitt nedenfor sammen med statistikken som er grunnlaget for figurene brukt i oppgaven.

Dagbladet
Derfor ble han frikjent for identitetstyveri
http://www.kjendis.no/2008/11/10/553490.html
Mobilsvindel, både tyveri og svindel

Anmelder moren for svindel

http://www.dagbladet.no/nyheter/2008/10/02/548938.html

Kredittsvindel, misbruk av navn og personnummer, bare svindel

Slik kan personnumrene misbrukes

http://www.dagbladet.no/nyheter/2008/09/17/547204.html

Misbruk av personnummer, bare svindel

Truet av ukjent

http://www.kjendis.no/2007/12/12/520996.html

Mobilsvindel, både svindel og tyveri

Noen har stjålet Jan Fredrik Karlsens identitet

http://www.kjendis.no/2007/11/27/519387.html

Adresseendring i folkeregisteret, mobilsvindel, misbruk av personnummer

Vil stanse identitetstyvene

http://www.dagbladet.no/dinside/2006/10/11/479414.html

Mobilsvindel

Dagfinn fikk kredittregning på 57 000

http://www.dagbladet.no/nyheter/2006/03/01/459390.html

Kredittsvindel

Bolighai tatt for kortsvindel

http://www.dagbladet.no/nyheter/2005/01/18/420615.html

Kredittsvindel

Mobilsjokk til en halv million

http://www.dagbladet.no/nyheter/2001/08/14/274633.html

Mobilsvindel

Korttyvene stjal mammas identitet

http://62.63.40.20/artikler/ident.htm

Adresseendring posten, adresseendring folkeregisteret, kredittsvindel

VG

Facebook-kontoer på billigsalg

http://www.vg.no/teknologi/artikkel.php?artid=545402

Tilegnelse av personopplysninger, identitetstyveri

Skrekkliste! Bærbare blemmer

http://www.vg.no/teknologi/artikkel.php?artid=527929

Personopplysninger på avveie, identitetstyveri

Stjeler identiteten din via IP-telefonen

http://www.vg.no/teknologi/artikkel.php?artid=520218

Salg av brukernavn og passord, identitetstyveri

Nordmenn likegyldige til IT-sikkerhet

http://www.vg.no/teknologi/artikkel.php?artid=519204

Sikkerhet i forhold til personopplysninger, tyveri av informasjon

Se opp for lotterisvindel på SMS

http://www.vg.no/teknologi/artikkel.php?artid=197706

Produksjon av falske papirer

Noen ser deg!

http://www.vg.no/teknologi/artikkel.php?artid=219384

Kredittsvindel, både tyveri og misbruk

Idol-Tone sjokkert over mobilstunt

http://www.vg.no/musikk/artikkel.php?artid=117258

Mobilsvindel

Neste generasjon nettsvindel

http://www.vg.no/teknologi/artikkel.php?artid=170838

Innsamling av personopplysninger ved bruk av ny teknologi, identitetstyveri

Kontantkort for netthandel

http://www.vg.no/teknologi/artikkel.php?artid=220591

Kredittsvindel, misbruk er identitetstyveri

Stadig flere svindles via e-post

http://www.vg.no/teknologi/artikkel.php?artid=6530882

Misbruk av navn

Nettavisen

Gikk til politiet med Haaviks identitet

http://www.nettavisen.no/innenriks/ioslo/article1737929.ece

Misbruk av identitetsbevis, kredittsvindel

”Gutten” nektet å ha gym

http://www.nettavisen.no/innenriks/ioslo/article1526084.ece

Misbruk av identitetsbevis

Dømt for brorens svindel

http://www.nettavisen.no/innenriks/article810974.ece

Misbruk av identitetsbevis

Kvinne fikk ID frastjålet

http://www.nettavisen.no/innenriks/article853282.ece

Kredittsvindel, både tyveri og misbruk

Lås postkassa

http://www.nettavisen.no/innenriks/article908709.ece

Kredittsvindel, både tyveri og svindel

Stor økning av identitetstyveri

http://www.nettavisen.no/innenriks/article801154.ece

Kredittsvindel, omadressering av post. Både svindel og tyveri

Du kan bli frastjålet id´en din
http://www.na24.no/arkiv/naeringsliv/article685962.ece
Mobilsvindel,

Kredittkortsvindel med mobil
http://www.nettavisen.no/it/article435729.ece
Kredittsvindel, både svindel og tyveri

Identitetstyveri største netttrussel
http://www.nettavisen.no/it/article363659.ece
Tyveri av personopplysninger

Han er landets huleste rektor
http://www.ba.no/nyheter/article4114891.ece
Misbruk av navn

Aftenposten
Knabber Iden din
http://www.aftenposten.no/nyheter/iriks/article2220545.ece
ID-tyveri er å stjele informasjon

Robber ID for millioner
http://e24.no/it/article1611147.ece
Kredittsvindel, ID-tyveri gjelder misbruk

Høysesong for kortsvindel
http://www.aftenposten.no/forbruker/pengenedine/article2526054.ece
Kredittsvindel, ID-tyveri gjelder misbruk

Avslør lotterisvindlerne
http://forbruker.no/pengenedine/article2269746.ece
Først stjele informasjon deretter begå identitetstyveri, kredittkortsvindel

Brøt seg inn i nettbank

http://forbruker.no/pengenedine/article2275970.ece

Kredittsvindel

Monsterhacking

http://e24.no/it/telekom/article1958133.ece

Innsamling er identitetstyveri

Ble ”forbryter” etter ID rot

http://www.aftenposten.no/nyheter/iriks/article2070218.ece

Misbruk av navn

Bankkort? Vis passet!

http://forbruker.no/pengenedine/article1662048.ece

Tilegnelse av identitetsbevis er identitetstyveri

Henlegger ID tyverier

http://www.aftenposten.no/nyheter/iriks/article1527432.ece

Mobilsvindel, bare misbruk

Hjulpet av DNBs internkontroll

http://www.aftenposten.no/nyheter/iriks/article1250102.ece

Kredittsvindel

Nordlys

Jeg vil ha nytt personnummer!

http://www.nordlys.no/debatt/ytring/article3795997.ece

Tyveri og misbruk av personsnummer

Sikrere å omadressere post

http://www.nordlys.no/nyheter/Innenriks/article3607844.ece

Tyveri

To tiltalt for grovt bedrageri

http://www.nordlys.no/nyheter/Innenriks/article826147.ece

Falske dokumenter

Sendte ut nesten fire millioner personnummre

http://www.nordlys.no/nyheter/article3791058.ece

Misbruk av personnummer

	Dagbladet	Nettavisen	Nordlys	VG	Aftenposten	
Typer av misbruk						
Kredittsvindel	4	5	0	2	5	16
Mobilsvindel	4	1	0	1	1	7
Dokumentfalsk	0	0	1	0		1
Misbruk av navn	1	1	0	1	1	4
Misbruk av personnummer	2	0	2	0		4
Adresseforandring Posten	1	1	0	0		2
Adresseforandring Folkeregisteret	2	0	0	0		2
Misbruk av identitetsbevis	0	3	0	1		4
	14	11	3	5	7	0

Tabell 4: Tilfeller av misbruk knyttet til identitetstyveri omtalt i media

	Dagbladet	Nettavisen	Nordlys	VG	Aftenposten	
Uberettiget tilegnelse av personopplysninger	8	1	1	5	3	18
Misbruk av personopplysninger	0	5	2	4	7	18
Begge deler	2	4	1	1	0	8
	10	10	4	10	10	0

Tabell 5: Hvordan mediene bruker begrepet identitetstyveri