



IDENTITETSMISBRUG



BELYST FRA FLERE VINKLER

Identitetsmisbrug belyst fra flere vinkler

April 2019

Forfatter: lektor Peter Kruise
Københavns Universitet, Det Juridiske Fakultet

Dette materiale er støttet økonomisk af Offerfonden og Det Kriminalpræventive Råd. Materialets udførelse, indhold og resultater er alene forfatterens ansvar. De vurderinger og synspunkter, der fremgår af materialet, er forfatterens egne og deles ikke nødvendigvis af Rådet for Offerfonden og/eller Det Kriminalpræventive Råd.

Denne publikation er kun udgivet som pdf på dkr.dk.

Kopiering tilladt med angivelse af kilde.

ISBN 978-87-985490-5-5

Forord

I 2009 skrev jeg en rapport om identitetstyveri. Det var den første forskningsrapport i Danmark om dette emne. Nu til dags er der en stigende opmærksomhed på identitetsmisbrug og internet-relateret kriminalitet, og i de sidste ti år er der kommet en hel del rapporter om emnet. De fleste studier er dog baseret på kvantitative offerundersøgelser, og der savnes en kvalitativ undersøgelse, som går mere i dybden med identitetsofrenes kamp mod misbruget og centrale aktørers oplevelse af identitetsmisbrug.

Det er derfor glædeligt, at Offerfonden har bevilget økonomisk støtte til netop et forskningsprojekt, der forsøger at komme hele vejen rundt om fænomenet identitetsmisbrug. Det Kriminalpræventive Råd har støttet en udvidelse af projektet med en tillægsbevilling.

Jeg vil gerne sige tak til alle, der har bidraget til dette projekt, det vil sige identitetsmisbrugsudsatte, som har stillet sig til rådighed for interviews, samt repræsentanter for virksomheder, myndigheder og organisationer. Jeg vil også gerne takke kontaktpersoner og respondenter i Norge, Holland og Storbritannien. Endelig vil jeg takke jurastuderende Helene Messmann, som har hjulpet med offerinterviews samt transskribering af interviewsamtaler.

Jægerspris

D. 5. april 2019

Peter Kruize

Indholdsfortegnelse

1. Indledning	7
1.1 Tilegnelse af identitetsoplysninger	8
1.2 Projektets formål og problemstillinger	11
1.3 Rapportens struktur	12
2. Metoder	13
2.1 Interviews med identitetsmisbrugsudsatte	13
2.2 Interviews med centrale aktører	15
2.3 Landestudier	19
3. Økonomisk misbrug	21
3.1 Misbrugte identitetsoplysninger	21
3.2 Metoder til at misbruge identitetsoplysninger (modus)	23
3.2.1 Køb, leje eller leasing af varer i fysiske butikker	24
3.2.2 Køb af varer i webbutikker	24
3.2.3 Pengeoverførsel i netbanken	25
3.2.4 Oprettelse af et forbrugslån (kviklån)	27
3.2.5 Oprettelse af en virksomhed	28
3.2.6 Modtagelse af strandet besked og CEO-bedrageri	29
3.2.7 Handelsbedrageri	30
3.2.8 Datingbedrageri	30
3.3 Offerprofil	31
3.3.1 Set med politiets øjne	31
3.3.2 Set med kreditorernes øjne	34
3.3.3 Set med hjælpernes øjne	35
4. Ærekrænkende misbrug	37
4.1 Overtagelse af udsattes profil eller konto	38
4.2 Oprettelse af en profil/konto med udsattes oplysninger	39
4.3 Uønsket deling og/eller manipulering af billeder/videoer	42
4.4 Offerprofil	44

5. Udsattes perspektiv	45
5.1 Opdagelse af identitetsmisbrug	46
5.2 Oprydningsarbejde	48
5.2.1 Politianmeldelse	48
5.2.2 Indsigelse	50
5.2.3 Spærring	51
5.2.4 Sletning af billeder, profiler og mere fra nettet	52
5.3 Konsekvenserne af identitetsmisbrug	53
5.3.1 Økonomiske konsekvenser	53
5.3.2 Psykiske konsekvenser ved økonomisk misbrug	53
5.3.3 Psykiske konsekvenser ved ærekrænkende misbrug	54
5.3.4 Syn på retssystemet	56
6. Aktørernes syn	57
6.1 Politianmeldelse	57
6.2 Efterforskning	60
6.3 Hæftelse for tabet	62
6.4 Sletning	64
7. Eksisterende tiltag	66
7.1 Er min identitet blevet misbrugt?	67
7.2 Nyt personnummer	68
7.3 Kreditadvarsel i CPR	70
7.4 Forsikring mod identitetstyveri	74
7.4.1 Økonomisk misbrug	75
7.4.2 Ærekrænkende misbrug	77
7.5 NGO'er	78
7.5.1 Mit Digitale Selvforsvar (Forbrugerrådet Tænk)	78
7.5.2 Den Sociale Retshjælps Fond	80
7.5.3 StopChikane (Dansk Kvindesamfund)	80
7.5.4 SletDet (Red Barnet)	81
8. Udenlandske lektioner	84
8.1 Definering og omfang af identitetsmisbrug i de undersøgte lande	84
8.1.1 Norge	84
8.1.2 Holland	86
8.1.3 Storbritannien	87

8.2 Identitetsmisbrug som særskilt paragraf i straffeloven	88
8.2.1 Danmark	89
8.2.2 Norge	91
8.2.3 Holland	93
8.3 Nationalt støttecenter	93
8.3.1 CMI i Holland.....	94
8.3.2 NorSIS i Norge.....	95
9. Konklusioner og overvejelser	97
9.1 Identitetsoplysninger	97
9.2 Instanser og dokumentationskrav	97
9.3 Psykiske konsekvenser	98
9.4 Økonomiske konsekvenser.....	99
9.5 Eksisterende tiltag	99
9.6 Udenlandske ordninger	100
9.7 Overvejelser	101
9.7.1 Særskilt lovparagraf	102
9.7.2 Spærring af identitetsbeviser	103
9.7.2 Nationalt center.....	103
Litteraturliste	104

1 Indledning

Digitaliseringen spiller nu til dags en central rolle for misbrug af identitetsoplysninger, men at sløre sin egen og/eller misbruge andres identitet har altid været en del af den kriminelle verden. Der er i Danmark gennemført adskillige undersøgelser af identitetstyveri (Kruize, 2009, 2013, 2015 og 2018), informationssikkerhed (Digitaliseringsstyrelsen og DKCERT, 2015) og digital tryghed (Forbrugerrådet Tænk, 2016). Disse studier kan betegnes som offerundersøgelser dækkende et repræsentativt udsnit af den danske befolkning med det primære formål at sætte tal på omfanget (kvantificering). Sideløbende ses med jævne mellemrum journalistiske indslag om ofre for identitetstyveri. Der savnes derimod en kvalitativ undersøgelse, som går i dybden med identitetsofrenes kamp mod misbruget og centrale aktørers oplevelse af identitetsmisbrug. Dette forskningsprojekt har til formål at udfylde dette hul i vores viden om identitetsmisbrug.

Kruize (2018, s. 30) påpeger, at først når selve misbruget af identitetsoplysninger opdages, bliver offeret klar over, at han eller hun har været udsat for en forbrydelse. Det antages f.eks., at det ikke er alle opsnappede cpr-numre, der benyttes efter et dataindbrud. Omfanget af dette mørketal er – ifølge sagens natur – ukendt. Dermed kan omfanget af identitetstyveri kun måles, når der er tale om viktimisering (fase 2 i skema 2.1). Først når identitetsoplysninger misbruges, er der et offer, som kan rapportere om det. Det er derfor mere korrekt at tale om omfanget af identitets*misbrug* (se også Wall, 2007; DKR, 2016). Kruize (2018) skelner mellem tre former for identitetsmisbrug:

- Misbrug af betalingskortoplysninger
- Misbrug af identitetsoplysninger med henblik på økonomisk gevinst
- Misbrug af personoplysninger med henblik på chikane mod offeret.

Misbrug af betalingskortoplysninger er den mest udbredte form for identitetsmisbrug. Ifølge den seneste offerundersøgelse har 2,5 % af den danske befolkning – svarende til godt 100.000 personer – været udsat for betalingskortmisbrug inden for de seneste 12 måneder (Kruize, 2018). Det økonomiske tab dækkes som regel af en tredjepart (f.eks. kortselskabet), og efter spærring af betalingskortet er problemet løst. Betalingskortmisbrug er dermed relativt omkostningsfrit for de umiddelbare ofre.

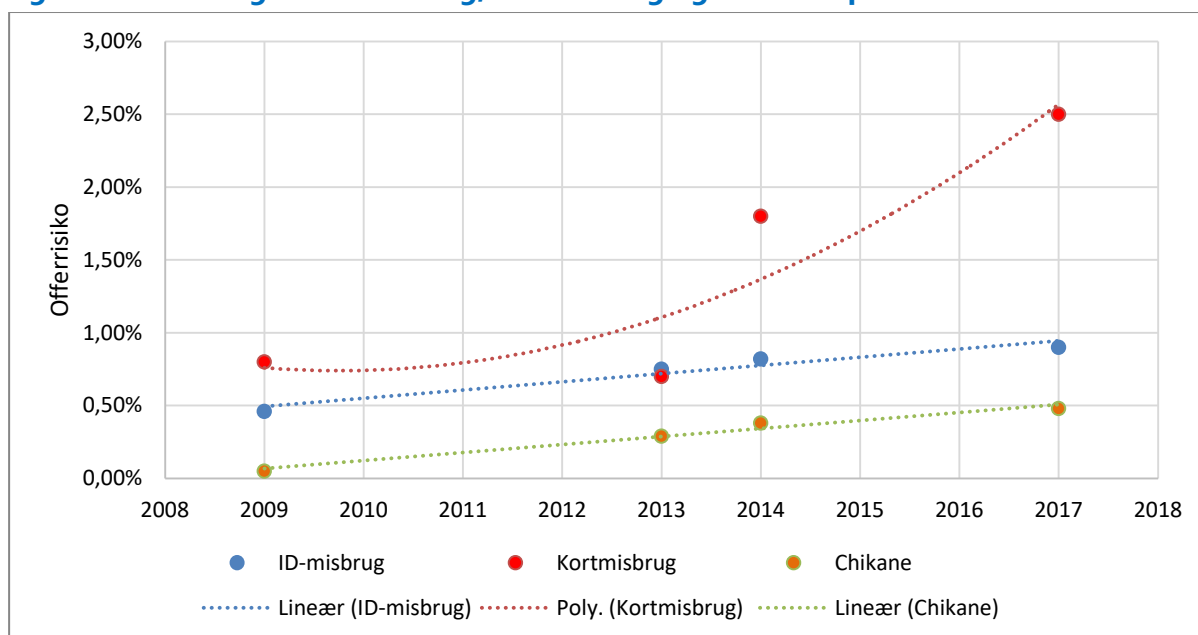
0,9 % af den danske befolkning har inden for de seneste 12 måneder været udsat for misbrug af identitetsoplysninger med henblik på økonomisk gevinst (Kruize, 2018), hvilket svarer til

knap 40.000 personer. Denne offerkategori omfatter dem, der f.eks. udsættes for, at en gerningsmand skaffer sig ulovlig adgang til deres bankkonti, bestiller varer eller opretter abonnementer i deres navn. For de fleste er skaden overskuelig, og hullet kan lukkes uden for meget besvær, men for et ukendt mindretal står misbruget på over længere tid og gør dagligdagen til et mareridt. Der har i pressen været flere eksempler på ofre, der har haft vanskeligt ved at få stoppet identitetsmisbruget.

Den tredje kategori af ofre for identitetsmisbrug – misbrug af personoplysninger med henblik på chikane – omfatter ifølge den seneste offerundersøgelse (Kruize, 2018) 0,5 % af den danske befolkning, godt 20.000 personer. Også her er der store variationer i misbrugets varighed og de gener, offeret udsættes for.

Misbrug af identitetsoplysninger, kortoplysninger og digitale profiler (chikane) var emnet for offerundersøgelserne i 2009, 2013, 2014 og 2017. Der findes således fire målinger for den forløbne niårsperiode. Figur 1.1 viser, hvordan disse tre former for misbrug af oplysninger knyttet til offerets person/identitet har udviklet sig. For både identitetsmisbrug og chikane er væksten mere eller mindre lineær.

Figur 1.1 Udviklingen i id-misbrug, kortmisbrug og chikane i perioden 2009-2017



Kilde: Kruize, 2018, s. 9.

1.1 Tilegnelse af identitetsoplysninger

Der er flere måder, hvorpå en gerningsperson kan tilegne sig andres (identitets)oplysninger. Offentligt tilgængelige registre, f.eks. telefon- og navneregistre, indeholder oplysninger som navn, adresse og telefonnummer. Internetsiden krak.dk er et eksempel herpå. Desuden læg-

ger privatpersoner ofte frivilligt personoplysninger ud på egne internetsider eller på sociale netværkssider som Facebook og LinkedIn. Oplysninger kan også blive franarret, f.eks. ved phishing, eller stjålet. En persons (identitets)oplysninger kan dermed falde i forkerte hænder på tre måder: frivillig fremlæggelse, bondefangeri eller tyveri.

Der kan skelnes mellem online- og offline-tilegnelse af (identitets)oplysninger. Online-tilegnelse knytter sig til internettet og det faktum, at når en enhed (computer, smartphone, tablet) tilsluttes nettet, er det muligt at trænge ind i den og/eller kommunikere med brugeren. Offline-tilegnelse betyder, at der er tale om en handling i den fysiske verden. Det kan dreje sig om lomme- eller tasketyveri, men kan dog også være af teknisk art, f.eks. skimming.

At franarre oplysninger (online) bliver ofte kaldt phishing (at fiske efter oplysninger). Formålet med phishing er at franarre offeret fortrolige oplysninger, typisk identitetsinformation og finansielle oplysninger. Phishing sker hyppigst ved, at en e-mail sendes til et stort antal adresser. For et par tusinde kroner kan en e-mail således afsendes til en million adresser. Modtagerne opfordres enten til at indtaste de ønskede oplysninger og sende e-mailen retur eller til at klikke videre til en phishing-side (pharming; det betyder, at brugeren videresendes til hjemmesider, som ser ægte ud, men i virkeligheden er falske).

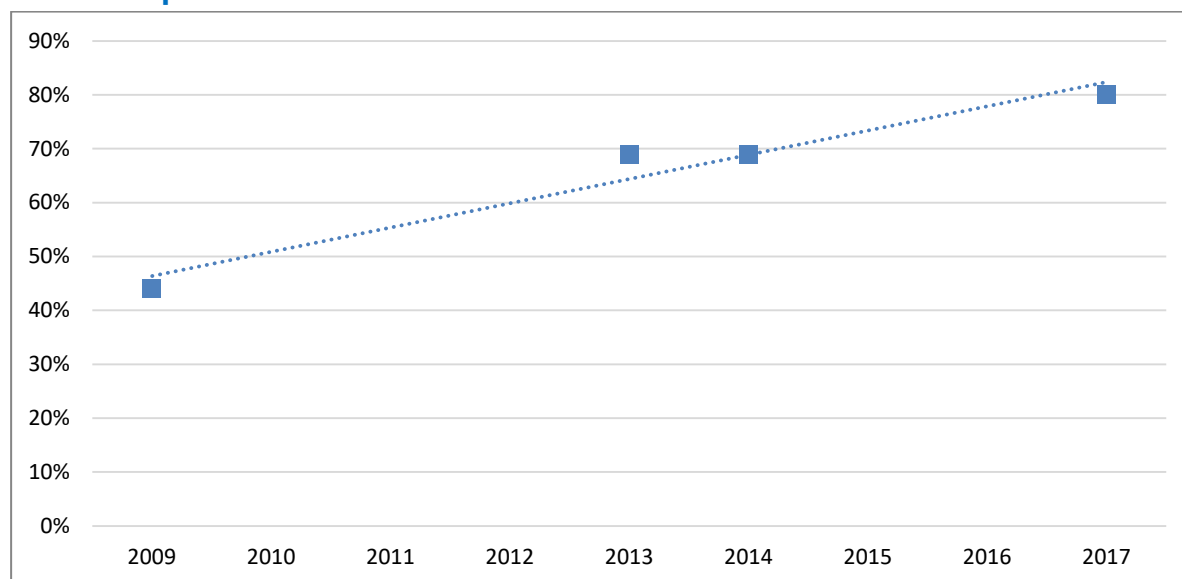
I undersøgelsen *Danskernes informationssikkerhed* (Digitaliseringsstyrelsen & DKCERT, 2017) blev der spurgt om, hvorvidt respondenter har modtaget e-mails med forsøg på phishing. 58 % svarede, at de har modtaget sådanne e-mails. Heraf har 5 % indsendt de efterspurgte oplysninger. 5 % af 58 % svarer til, at ca. 3 % af de udspurgte borgere har været udsat for phishing. Eftersom spørgsmålet ikke indeholdt en tidsbegrænsning, er det uvist, hvor mange der har været udsat for phishing på årsbasis.

Når en enhed (computer, smartphone, tablet) tilsluttes internettet, kan den kommunikere med omverdenen. Bagsiden er, at enheden kan angribes af andre brugere. Den mest kendte form for angreb er computervira. En computervirus er et lille program, der forsøger at inficere andre programmer. Oftest synes programmet harmløst, og det skal aktiveres manuelt for at kunne indlede spredningen. Virusprogrammer kan være meget skadelige, f.eks. kan de slette vigtige data og/eller programfiler fra den inficerede computer. De fleste brugere har udstyret deres computer med et antivirusprogram. Men som nævnt er computervira langt fra de eneste programmer, hvormed en computer kan inficeres. Listen er lang, og alle disse programmer hører under betegnelsen *malware*. Malware er en sammentrækning af de engelske ord *malicious software* (på dansk: ondsindet programkode). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på.

I DKCERT Trendrapport 2017 oplystes fordelingen af malware, som antivirusproducenten F-Secure havde identificeret på danskernes computere. Trojanske heste¹, der typisk spredes via inficerede websteder og e-mails, var i 2016 stadig klart den største malware-trussel. Trojanske heste stod således for 89 % af alle konstaterede trusler; en mindre stigning i forhold til 2015, hvor de tegnede sig for 84 %. Den mest udbredte trojanske hest i Danmark i 2016 var JS/Kavala, typisk sendt i en e-mail med en vedhæftet fil (DKCERT Trendrapport 2017, s. 13). En undersøgelse i regi af Digitaliseringsstyrelsen & DKCERT udført i 2016 viste, at 31 % af alle danskere har haft virus eller andre former for skadelige programmer i deres computer.

I offerundersøgelser om identitetstyveri (Kruize, 2009, 2013, 2015 og 2018) er respondenterne, som har været udsat for misbrug af identitets- eller betalingskortoplysninger, blevet spurgt om, hvorvidt de ved, hvordan gerningspersonen har fået fat i deres oplysninger. Med årene er der færre, der svarer, at de har en formodning om, hvordan gerningspersonen har fået fat i deres oplysninger. I 2009 svarede 80 %, at de havde en formodning. I 2013 var det kun halvdelen, mens procentdelen faldt til 28 i 2017. En forklaring på dette fænomen kan være, at vi bevæger os mere og mere i cyberspace, og at det dermed er blevet vanskeligere at have en idé om, hvor og hvordan gerningspersonen har tilegnet sig oplysninger. Ovenstående antagelse er konsistent med svarene af respondenter, der har en formodning om, hvordan gerningspersonen har fået kendskab til deres oplysninger. Andelen af respondenter, der peger på online-tilegnelse, er næsten fordoblet i perioden 2009-2017 (se Figur 1.2).

Figur 1.2 Andelen af ofre for identitets- og kortmisbrug, hvis oplysninger er blevet stjålet online i perioden 2009-2017

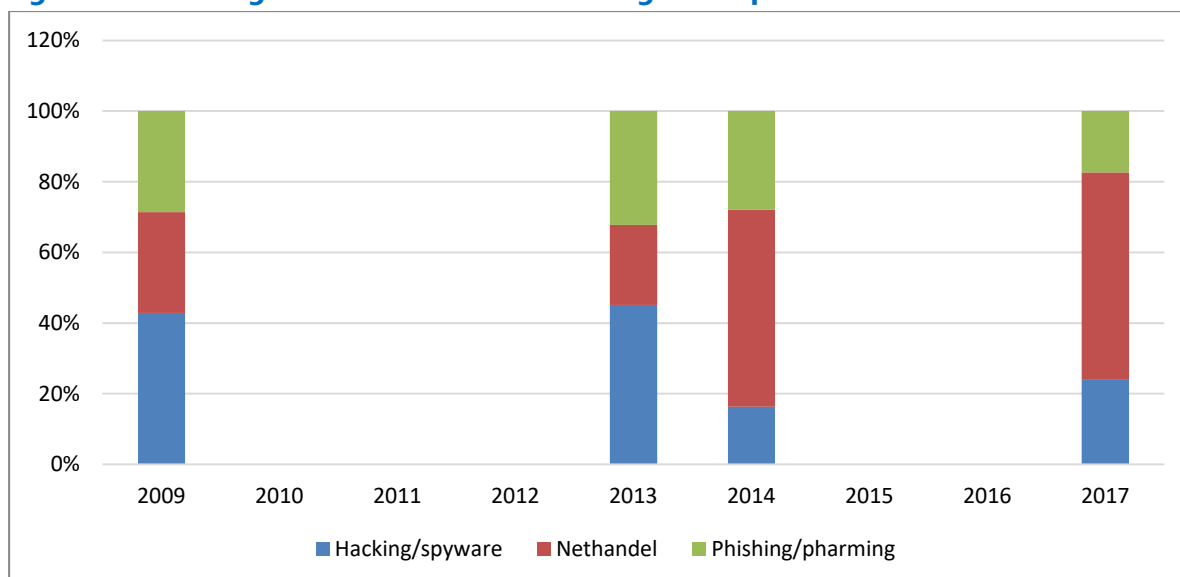


Kilde: Kruize, 2009, 2013, 2015 og 2018.

¹ En trojansk hest er malware forklædt som noget harmløst. Trojaneren er ofte et serverprogram, der gør det muligt at fjernstyre den smittede enhed. Det kaldes derfor også at installere en bagdør. Adgangen kan fx misbruges til at foretage DDoS-angreb mod andre systemer på internettet.

De respondenter, der har været udsat for et online-tyveri af deres identitetsoplysninger, er også blevet spurgt om, hvorvidt de har en formodning om, hvordan gerningsmanden har fået fat i deres oplysninger. Når vi ser på tendensen over tid, peger flere og flere udsatte på, at de har mistet deres oplysninger – specielt kortoplysninger – i forbindelse med handel på nettet (se Figur 1.3).

Figur 1.3 Fordelingen af online-former for tilegnelse i perioden 2009-2017



Kilde: Kruize, 2009, 2013, 2015 og 2018

1.2 Projektets formål og problemstillinger

Som sagt savnes en undersøgelse, som går i dybden med identitetsofrenes kamp mod misbruget og de centrale aktørers oplevelse af identitetsmisbrug. Dette forskningsprojekt har bl.a. til formål at udfylde dette hul i vores viden om identitetsmisbrug. Et andet formål er at se nærmere på de eksisterende muligheder for at få støtte ved identitetsmisbrug samt på behovet for yderligere tiltag. Der ses nærmere på seks problemstillinger:

1. Hvilke identitetsoplysninger danner typisk grundlag for (langvarigt) misbrug?
2. Hvilke instanser (offentlige og private) skal informeres, når man vil gøre sig fri af identitetsmisbrug, og hvilke dokumentationskrav stiller disse instanser til ofrene?
3. Hvilke psykiske konsekvenser har (langvarigt) identitetsmisbrug for ofrene, og i hvilken grad benytter disse sig af psykologisk bistand?
4. Hvilke (indirekte) økonomiske følger har (langvarigt) identitetsmisbrug for ofrene, og i hvilken grad kompenseres disse?
5. Hvilke tiltag savner ofrene i kampen mod misbruget?
6. Hvordan støttes ofrene i Norge, Holland og Storbritannien, og har disse lande ordninger, der med fordel vil kunne anvendes i Danmark?

1.3 Rapportens struktur

Der redegøres for de anvendte forskningsmetoder i kapitel 2. Efterfølgende introduceres to typer af identitetsmisbrug: økonomisk misbrug (kapitel 3) og ærekrænkende misbrug (kapitel 4). I disse kapitler beskrives de mest anvendte former for misbrug inden for de to kategorier, og der tegnes en profil af, hvem der bliver udsat for identitetsmisbrug.

Fænomenet identitetsmisbrug belyses fra to sider; fra de udsattes side (kapitel 5) og fra aktørernes side (kapitel 6). I disse kapitler ses der nærmere på de forskellige aktiviteter i forbindelse med og konsekvenserne af identitetsmisbrug.

I kapitel 7 beskrives de eksisterende tiltag til gavn for identitetsmisbrugsudsatte i Danmark, og i hvilken grad udsatte er bekendt med/benytter disse tiltag. I kapitel 8 ses der nærmere på, hvilke tiltag der findes i Norge, Holland og/eller Storbritannien, og som kunne være interessante i en dansk kontekst. Rapporten afsluttes med konklusioner og overvejelser (kapitel 9).

2 Metoder

For at kunne opfylde forskningsprojektets formål er der anvendt en række metoder til at indsamle relevante oplysninger. Ved siden af desk research – det vil sige litteratursøgning, besøg på relevante hjemmesider, chatfora og brug af (offentligt) tilgængelige statistiske oplysninger² – er der afholdt interviewsamtaler med identitetsmisbrugsudsatte og repræsentanter for centrale aktører, ligesom der er udført landestudier. Herunder redegøres for disse metoder.

2.1 Interviews med identitetsmisbrugsudsatte

For at kunne afklare, hvordan ofre for identitetsmisbrug har forsøgt at slippe fri af misbruget, hvilke instanser de har kontaktet, og hvordan de har oplevet hjælpen (eller manglen på samme), er der gennemført kvalitative interviews med identitetsmisbrugsudsatte. Interviewene er optaget digitalt, transskriberet og analyseret.

I første omgang har vi forsøgt at rekruttere interviewrespondenterne gennem en websurvey. Der er udarbejdet en websurvey i SurveyXact – et redskab fra Rambøll, der kan benyttes af medarbejdere på Københavns Universitet. Projektets formål er omtalt på Det Juridiske Fakultets og Forbrugerrådet Tænks Facebook-sider med et link til spørgeskemaet. Skemaet har været online fra d. 13. marts 2017 til og med d. 10. juli 2017. I denne periode har 157 personer klikket på linket til spørgeskemaet. Kun otte personer har udfyldt spørgeskemaet, og af disse otte personer svarer tre, at de har været udsat for identitetsmisbrug. Ingen af respondenterne har indikeret, at de vil stille op til interview.

En websurvey har vist sig at være en blind vej i forhold til rekruttering, og vi har derfor med held afprøvet andre metoder. Først har vi søgt på internettet efter personer, der omtaler sig selv eller bliver omtalt som identitetsmisbrugsudsatte. Udsatte kommer til orde i journalistiske indslag i aviserne og i fjernsynet (DR- og TV2-kanalerne), og der findes en Facebook-gruppe ved navn 'ID-tyveri i Danmark'. Vi udarbejdede derfor en liste med 47 personer, der har været skrevet om, og/eller som har fortalt om deres oplevelse. Vi har forsøgt at komme i kontakt med disse personer. Langtfra alle var til at opspore, og enkelte havde ikke lyst til (igen) at stille op til interview. I alt har vi gennemført et (telefonisk) interview med 23 af disse personer. Selvom de optræder med deres navn i de oprindelige journalistiske indslag, har vi valgt at anonymisere dem. I forhold til de oprindelige interviews gav vores egne interviews

² CPR-kontoret har stillet oplysninger til rådighed angående kreditadvarsel.

svar på flere spørgsmål, men kernen af mediehistorierne viser sig at være ret præcise. Dermed kan historierne om dem, vi ikke har talt med, formentlig også betragtes som troværdige.

Der må være en grund til, at en person søger medieopmærksomhed eller deler sin oplevelse på en eller andet internetplatform. Gennemlæsning af historikken for Facebook-gruppen 'ID-tyveri i Danmark' giver indtryk af, at der er to overvejende grunde til, at udsatte skriver et indslag.³ Der er en del personer, der vil dele deres oplevelse med henblik på at advare andre eller give gode råd om, hvordan man håndterer sådan en sag, og sikkert samtidig komme af med deres frustration over, hvad der er sket eller sker. Og så er der udsatte, der søger hjælp hos andre medlemmer af gruppen: Hvad kan eller bør de gøre i en bestemt situation?⁴

Vi har også forsøgt at inddrage interviewrespondenterne i undersøgelsen gennem en anden rekrutteringsmetode. Vi har således bedt Københavns Politi om at kontakte anmeldere af identitetsmisbrug, og politiet sendte derefter d. 21. november 2017 en e-mail til 25 udvalgte anmeldere og spurgte om, hvorvidt de var interesserede i at deltage i undersøgelsen. I givet fald opfordredes de til at kontakte forskeren. Denne opfordring førte til to interviewsamtaler. Formentlig var det faktum, at anmelderne af identitetsmisbrug selv skulle tage kontakt til forskeren, et væsentligt minus ved denne rekrutteringsmetode. Københavns Politi havde imidlertid ikke ressourcer til at kontakte anmelderne telefonisk for at høre, om de ville deltage i undersøgelsen, og man ville ikke have, at udefrakommende kontaktede anmelderne.

Det er svært at fastslå, hvor repræsentative interviewrespondenterne er i forhold til identitetsmisbrugsudsatte. Ved kvalitative interviews sigtes der heller ikke efter repræsentativitet, men efter at 'mætte' kategorierne. Det er heller ikke nødvendigvis problematisk, at der er gennemført færre interviewsamtaler end oprindeligt planlagt. Også 25 samtaler kan være nok til at opnå indsigt i problematikken. Historierne om de 24 udsatte, omtalt i journalistiske indslag eller delt på nettet, som ikke ville stille op til interview eller ikke kunne kontaktes, afviger ikke fra det billede, der kommer frem på basis af de 25 gennemførte interviews. Det betrag-

³ Facebook-gruppen 'Identitetstyveri i Danmark' er oprettet d. 13. juni 2013 af Henriette Thiim, som selv har været udsat for identitetsmisbrug og har optrådt i adskillige journalistiske indslag om sin egen sag. Hun beskriver gruppen således: "En gruppe for personer som har været udsat for identitetstyveri. Det er meget svært at stoppe misbruget, da hverken kørekort eller sygesikringsbevis kan spærres effektivt som et betalingskort kan. Det er meget let at oprette forbrugslån med et kørekort og et sygesikringsbevis. Ofrenes cpr-nr. må ifølge persondataloven ikke registreres hos Experian eller Debitorregistret. Det er næsten umuligt at stoppe fortsat misbrug". Efterfølgende giver hun en lang liste med råd til, hvad identitetstyverudsatte kan gøre for at stoppe misbruget.

De sidste par år er der dog ikke sket ret meget mere i gruppen. De fleste indslag af nyere dato er fra journalister eller studerende på Journalisthøjskolen, som søger identitetsmisbrugsudsatte, som vil stille op til interview.

⁴ Udover indslag om medlemmernes egne erfaringer diskuteres også de adskillige (politiske) tiltag, der løbende er indført.

tes som et tegn på, at dobbelt så mange interviews (som var ambitionen) ikke ville have ført til andre indsigter.

Der er 15 mænd og 10 kvinder blandt de 25 interviewede personer. De fleste har været udsat for identitetsmisbrug med et økonomisk sigte, mens 9 personer har været ofre for ærekrænkende identitetsmisbrug, muligvis med henblik på chikane.

Der mangler dog interviewrespondenter, som repræsenterer, hvad der ofte betegnes som 'svage borgere'. Adskillige repræsentanter for centrale aktører peger på denne type offer, og på websiden www.ligevaerd.dk påpeges det, at "Den seneste tid har der i pressen været fokus på unge med særlige behov, der har været udsat for identitetstyveri og er blevet svindlet for store summer". Også andre kategorier af 'svage borgere' – hjemløse og dem, der er en del af misbrugsmiljøet – mangler blandt interviewrespondenterne. Der, hvor dette emne omtales i rapporten, inddrages mediehistorier og beretninger fra centrale aktører.

2.2 Interviews med centrale aktører

Der er en hel del offentlige instanser og private virksomheder, der har en aktie i fænomenet identitetsmisbrug. Det kan være, at de står for eller burde stå for en hjælpende hånd, men det kan også være, at de repræsenterer den krævende part. I alt er der gennemført 29 interviews med repræsentanter for centrale aktører. Det er dog ikke lykkedes at komme i kontakt med et antal private virksomheder, som kan anses for at være vigtige aktører. Herunder redegøres der for de gennemførte interviews samt for de forsøg, som ikke har ført til en samtale eller en udtalelse.

Politiet

Politiet er en vigtig instans for identitetsmisbrugsudsatte. Bortset fra at mange udsatte vil prøve at søge hjælp hos politiet, kræver kreditorerne ofte, at sagen anmeldes til politiet. Rigspolitiets National Cyber Crime Center (NC3) har det overordnede ansvar for identitetsmisbrug, men anmeldelser skal indgives lokalt, ligesom efterforskning i princippet finder sted i lokalt regi. Identitetsmisbrug med et økonomisk sigte varetages af en afdeling for økonomisk kriminalitet i landets politikredse⁵, mens ærekrænkende identitetsmisbrug overvejende hører hjemme under almen efterforskning.

⁵ Siden januar 2019 findes LCIK. LCIK står for Landsdækkende Center for It-relateret økonomisk Kriminalitet. Det er forankret under Københavns Politi, men varetager sager i hele landet. LCIK modtager elektroniske anmeldelser af internetsvindler og står for den indledende efterforskning. Efterfølgende sendes såkaldte sagspakker ud til de retmæssige kredse, som fortsat skal stå for at oprette sigtelser. Ifølge politiet skal det gøre arbejdet mere fokuseret og samlet og lette arbejdsbyrden i de lokale kredse.

Vi har sendt en opfordring til en interviewsamtale til alle tolv politikredse samt NC3. Otte af de tolv kredse har stillet op til en (telefonisk) interviewsamtale.⁶ I syv kredse er der blevet gennemført en telefonisk interviewsamtale med en leder af afdelingen for økonomisk kriminalitet eller IT-kriminalitet, og i tre af disse kredse er der også blevet afholdt et telefonisk interview med en leder af almen eller lokal efterforskning. I Københavns Politikreds er der blevet gennemført personlige interviews med repræsentanter for sagsvisitationen og to forebyggelseskonsulenter samt en telefonisk samtale med en leder for almen efterforskning. Endelig er der afholdt et personligt interview med en sektionsleder for NC3. Det betyder, at der i alt er blevet afholdt 13 (telefoniske) interviews med politirepræsentanter.

Pengeinstitutter

Når det handler om identitetsmisbrug med et økonomisk sigte, kan der i teorien være tre parter, der hæfter for tabet. Personen, der har været udsat for identitetsmisbrug⁷, pengeinstituttet eller virksomheden, der har leveret en ydelse eller vare. Når det handler om et pengeinstitut, kan der være tale om en bank, en udbyder af betalingskort eller en udbyder af kortfristede forbrugslån – ofte betegnet som kviklån.

Der er blevet afholdt et telefonisk interview med en kontorchef i Finans Danmark⁸, et personligt interview med en bankdirektør (Basisbank⁹) og et personligt interview med en direktør hos en udbyder af digitale forbrugslån (4Finance¹⁰). Den sidste interviewrespondent er også bestyrelsesmedlem i Dansk Kredit Råd.¹¹

⁶ Tre politikredse har ikke reageret på opfordring og reminder til en interviewsamtale: Syd- og Sønderjylland, Midt- og Vestsjælland og Bornholm. Østjyllands Politikreds henviste til Nationalt Forebyggelses Center (NFC). En efterfølgende e-mail om, at jeg gerne ville tale med en repræsentant for politikredsen (og hvorfor), blev ikke besvaret.

⁷ Eller påstår, at han/hun har været udsat for identitetsmisbrug. Til dette spørgsmål vendes tilbage senere i rapporten.

⁸ Finans Danmark er interesseorganisation for banker, realkreditinstitutter, kapitalforvaltning, værdipapirhandel og investeringsfonde i Danmark (www.finansdanmark.dk).

⁹ "Forretningsmodellen er at drive en nemt tilgængelig internetbank, med enkle indlånsprodukter og usikrede forbrugslån. Usikrede forbrugslån udbydes online via forskellige brands såsom "LånLet", "Selenes Finans" og "Nupp". Banken samarbejder ligeledes med en række bilforhandlere, detailhandlere og webbutikker mv., hvor usikrede forbrugslån tilbydes i forbindelse med køb af varer og tjenester. Banken er alene aktiv på det danske marked" (Årsrapport 2017, s. 10; downloaded fra www.basisbank.dk).

¹⁰ 4Finance er en af Europas største online-lånevirksomheder, som tilbyder lån og kreditter med hurtig udbetaling (kviklån). I Danmark har 4Finance to produkter, VIVUS.DK og Zaplo.dk. Der har været en del mediekritik af 4Finance og dens russiske ejer Oleg Bojko; se fx følgende artikel i Politiken:

<https://politiken.dk/forbrugogliv/art5958097/Russisk-milliard%C3%A6r-tjener-tykt-p%C3%A5-danskere-som-lader-sig-friste-af-hurtige-l%C3%A5n>

¹¹ Dansk Kredit Råd er en forening, der virker som et fagligt og personligt netværk for virksomheder og personer, der arbejder professionelt med kreditgivning (www.dk-r.dk).

(Web)butikker

Som sagt kan virksomheder, der har leveret en ydelse eller en vare, hæfte for (en del af) tabet på grund af identitetsmisbrug. Der er søgt kontakt til seks store butikskæder i kategorierne supermarked (Coop¹² og Dansk Supermarked Group¹³), elektronik (Elgiganten¹⁴), telekommunikation (TDC Group¹⁵ og Telia¹⁶) og leasing (L'EASY¹⁷). Vi har skrevet/ringet til presseafdelingerne, og en af dem har sendt min opfordring videre til den juridiske afdeling (TDC Group). Efter flere rykkere måtte jeg opgive at komme igennem. Tre butikskæder har ikke svaret (Coop, Elgiganten og Telia), heller ikke efter rykkere. Der blev gennemført telefoniske interviews med repræsentanter for Dansk Supermarked Group og L'EASY.

Desuden har vi forgæves forsøgt at komme i kontakt med Dansk Erhverv og Foreningen for Dansk Internet Handel (FDIH).

Inkassovirksomheder

Når kreditorerne holder fast i deres krav, kan de sende fordringen videre til en inkassovirksomhed. I sidste instans kan sagen ende i fogedretten. Jeg har skrevet til to virksomheder, der (også) beskæftiger sig med inkasso (Advokaternes Inkasso Service¹⁸ og Debito¹⁹). Disse to virksomheder har svaret på e-mail. Via en anden respondent kom jeg i kontakt med en af de større inkassovirksomheder i Danmark (Collectia²⁰), hvilket førte til et personligt interview samt et interview med en partner i advokatkontoret Lund Elmer Sandager²¹, som har specialiseret sig bl.a. i inddrivelse af gæld.

¹² Coop Danmark A/S er en detailhandelsvirksomhed i Danmark med en markedsandel på 38 %. Coop står bag Kvickly, SuperBrugsen, Dagli'Brugsen, Irma og Fakta samt e-handelsbutikken coop.dk.

¹³ Dansk Supermarked Group har i maj 2018 skiftet navn til Salling Group. Salling Group står bag Føtex, Bilka, Netto, Salling og Wupti.

¹⁴ Elgiganten er en varehuskæde inden for forbrugerelektronik og hårde hvidevarer. I Danmark er kæden markedsledende.

¹⁵ TDC Group er moderselskabet for YouSee, TDC Erhverv, Dansk Kabel TV, Telmore, Fullrate, Blockbuster, Netdesign og Get.

¹⁶ Telia Danmark hører under Telia Company med hovedsæde i Stockholm. Telia er den tredjestørste udbyder af telecom-services på det danske marked.

¹⁷ L'EASY udlejer langvarige forbrugsgoder og hører, sammen med Inspiration og D:E:R, under 3C Retail, som er en del af 3C Holding, ejet af den fynske rigmand Niels Thorborg.

¹⁸ Advokaternes Inkasso Service er en del af Advokatfirmaet Stohn (www.inkassoadvokat.dk).

¹⁹ Debito er en online-inkassotjeneste (www.debito.dk).

²⁰ Collectia A/S blev etableret på det danske marked i 1998 under navnet Transcom CMS A/S. Transcom blev til Collectia, efter opkøb af virksomheden i 2016 af kapitalfonden Findos Gmbh (www.collectia.dk).

²¹ Lund Elmer Sandager er et advokatfirma med fokus på rådgivning om erhvervsmæssige forhold og erhvervsrelateret lovgivning. Lund Elmer Sandager hører til blandt de større danske advokatfirmaer (www.les.dk).

Forsikringsselskaber

For nogle år siden begyndte forsikringsselskaber at tilbyde dækning ved identitetstyveri som del af kundernes familieforsikring. Senere er denne service blevet udvidet med Websikring, hvis kunden er udsat for chikane på nettet. Hvad disse forsikringer dækker, vender jeg tilbage til senere i rapporten. Jeg har skrevet til Tryg og Codan om deltagelse i projektet, men uden resultat. Der har været en e-mailkorrespondance med Top Danmark om, hvor ofte og hvilke type af henvendelser de modtager.

Det viser sig, at flere større og mindre forsikringsselskaber har udliciteret rådgivning og sagsbehandling til Affinion. Det betyder, at den reelle kontakt med forsikringskunder, der har været udsat for identitetsmisbrug, finder sted med en Affinion-medarbejder. Der er blevet afholdt en personlig interviewsamtale med to repræsentanter for Affinion og en sagsbehandler, som var med på en telefonisk forbindelse fra Oslo. Senere har jeg besøgt Affinions lokaler i Oslo under besøget i Norge (se også under landestudier).

Amerikanske internetgiganter

Når det handler om ærekrænkende identitetsmisbrug, spiller udbydere af sociale medier og internetsøgemaskiner en vigtig rolle ved at fjerne profiler og henvisninger i søgeregistret, samt ved at bidrage til efterforskningen, hvis en sag efterforskes af politiet. Vi har forsøgt at komme i kontakt med to dominerende spillere: Facebook og Google. På begge virksomheders hjemmesider står en vejledning i, hvordan en person kan anmode om sletning, når der er tale om identitetsmisbrug (hertil vender jeg tilbage senere i rapporten). Men det oplyses ikke, hvordan man kommer i kontakt med den danske afdeling af virksomheden. Der oplyses hverken telefonnumre eller e-mailadresser. Der kan kun skrives til USA. Det har jeg så gjort, men uden resultat.

Efterfølgende har jeg forsøgt at finde ud af, om der findes en repræsentant fra Facebook og Google. Det lykkedes at finde frem til navne. Jeg har forsøgt at komme i kontakt med dem både pr. e-mail og på LinkedIn, men uden resultat.

NGO'er

Der er adskillige NGO'er, der på en eller anden måde støtter udsatte for identitetstyveri. Der har været kontakt med Forbrugerrådet Tænk (www.taenk.dk). Det er en medlemsorganisation med mere end 82.000 personlige medlemmer og 28 medlemsorganisationer og forbrugergrupper. Forbrugerrådet Tænk har i flere omgange haft identitetstyveri på dagsordenen. De står bag undersøgelsen Digital Tryghed (2016), som er udarbejdet med støtte fra TrygFonden, samt app'en Mit Digitale Selvforsvar, som blev lanceret i april 2017 i samarbejde med Det Kriminalpræventive Råd og TrygFonden. Denne app bliver omtalt nærmere i afsnit 7.5.

Der har også været kontakt med Dansk Kvindesamfund (www.danskkvindesamfund.dk), som er en NGO, der kæmper for ligestilling mellem kønnene. Dansk Kvindesamfund står – med støtte af Offerfonden – bag initiativet StopChikane. StopChikane er et tilbud til voksne, der har fået delt billeder uden samtykke. Der ydes gratis rådgivning i, hvordan billeddelingen dokumenteres, hvordan og hvornår den anmeldes til politiet, og hvordan konsekvenserne håndteres, og yderligere deling stoppes. Dette initiativ bliver omtalt nærmere i afsnit 7.5.

Red Barnet (www.redbarnet.dk) er den danske afdeling af organisationen Save the Children, som er aktiv i mere end 120 lande. I Danmark bekæmper Red Barnet mobning, vold og seksuelle overgreb og fattigdom. Red Barnet står i samarbejde med Det Kriminalpræventive Råd bag initiativet SikkerChat. SikkerChat handler om sikker adfærd på nettet. Der er udviklet materiale rettet mod unge og deres forældre samt undervisningsmateriale. En del af SikkerChat er SletDet, som rådgiver unge i forhold til grænseoverskridende eller krænkende billeder eller videoer på nettet. Også dette initiativ omtales nærmere i afsnit 7.5.

Endelig har der været kontakt med en repræsentant for Den Sociale Retshjælps Fond (DSRF) (www.socialeretshjaelp.dk). Den Sociale Retshjælp blev i 2007 stiftet som en forening baseret på frivillighed, og i 2014 overgik foreningen til en fond med støtte fra Grundfos. DSRF yder bl.a. gratis juridisk rådgivning og gældsrådgivning til socialt udsatte og øvrige borgere under indtægtsgrænsen for fri proces. DSRF har 160-180 medarbejdere, hvoraf langt de fleste er frivillige og ulønnede praktikanter, som i perioder er tilknyttet organisationen som en del af deres studieordning. De yder også bistand til identitetsmisbrugsudsatte. DSRF omtales nærmere i afsnit 7.5.

2.3 Landestudier

Vi har valgt at se nærmere på erfaringerne med identitetsmisbrug i Norge, Holland og Storbritannien. Valget af Norge og Holland er begrundet af, at disse lande kan betragtes som sammenlignelige med Danmark. Norge har, som det første land i Skandinavien, indført en selvstændig bestemmelse om identitetsmisbrug (krænkelse) i straffeloven. Det gælder også for Holland. Ved siden af det findes der i Holland et nationalt center i myndighedsregi for identitetsmisbrugsudsatte. Udviklingen af bedrag på internettet ser ud til at være længere fremme i USA og andre engelsktalende lande – formentlig på grund af sproget – og dermed var det oplagt at se nærmere på situationen i Storbritannien. Storbritannien har en stærk tradition for forskning, og mange kriminalpræventive initiativer stammer herfra.

De tre lande er blevet besøgt; Holland fra d. 17. til og med d. 19. maj 2017, Norge fra d. 12. til og med d. 16. februar 2018 og Storbritannien fra d. 15. til og med d. 19. oktober 2018. Under disse besøg har der været interviewsamtaler med repræsentanter for politiet, hjælpeorgani-

sationer og forskere. Forud for et landebesøg er der blevet udført søgninger på nettet efter statistikker, forskning, iøjnefaldende initiativer, lovparagraffer og (juridisk) argumentation.

3 Økonomisk misbrug

I dette kapitel ses der nærmere på, hvilke personoplysninger der bliver anvendt ved økonomisk misbrug (3.1), på hvilken måde disse oplysninger bliver udnyttet (3.2), og til sidst hvem der typisk bliver udsat for økonomiske former for identitetsmisbrug (3.3).

3.1 Misbrugte identitetsoplysninger

Det kan være alle mulige personoplysninger, der muligvis er interessante til at udføre en eller anden form for identitetsmisbrug. Når man henvender sig telefonisk eller personligt til en myndighed eller virksomhed, bliver der ofte stillet et eller flere personlige spørgsmål med henblik på at finde ud af, om man er den, man hævder. Det kan f.eks. være ens postnummer eller adresse, men kan også være svaret på et spørgsmål, man har besvaret, da man oprettede kontoen, kortet eller lignende – f.eks. navnet på ens hund, fars/mors fødselsdato osv. Meget baggrundsviden om en person kan samles på de sociale medier.

I Danmark identificerer man typisk sig selv med sit personnummer – cpr-nummeret.²² Når vi går nogle år tilbage i tiden, kunne ens identitet misbruges blot ved brug af cpr-nummeret. Der kunne bestilles varer, oprettes abonnementer osv. udelukkende med et personnummer.

I en sag fra 2010 blev en kvindes personnummer misbrugt til at oprette flere mobiltelefonabonnementer samt benzin- og videokort i hendes navn. Identitetstyven fik også gennemført en adresseændring, og kvinden opdagede først misbruget, da hun blev kontaktet af sit forsikrings-selskab i forbindelse med hendes 'flytning'.

I langt de fleste tilfælde er det ikke længere muligt. Forhandlere og myndigheder har strammet op, og et personnummer er ikke mere tilstrækkeligt til at oprette et abonnement eller gennemføre et køb. Der kræves en form for (billed)legitimation – ved fysisk tilstedeværelse –

²² Et cpr-nummer er et personligt identifikationsnummer, som gives til statsborgere og borgere med opholdstilladelse i Danmark samt borgere, der er bosat uden for Danmark, men er medlem af ATP eller er skattepligtige efter skattekontrollen. Cpr-nummeret blev indført ved folkeregisterloven i 1968 og på Grønland i 1972. Nummeret består af ti cifre, hvoraf de første seks angiver fødselsdatoen, og de næste fire er et løbenummer, altså et nummer, som forøges løbende med udstedelsen af nye personnumre. Det 10. ciffer i personnummeret angiver personens køn. Hvis tallet er lige, er det en kvinde, og hvis tallet er ulige, er det en mand.

eller NemID-validering. NemID blev introduceret i 2010, og efterhånden anvendes NemID-validering af flere og flere offentlige tjenester og private (salgs)kanaler. Det er dermed ikke overraskende, at gerningsmandens fokus er flyttet fra personnummer til NemID.²³

Der er fire identitetsdokumenter, der ofte bliver nævnt i forbindelse med identitetsmisbrug. For det første er der danskernes officielle legitimationsbevis – passet. De fleste borgere går ikke rundt med deres pas til daglig – i modsætning til kørekort og sundhedskort – men alligevel meldes mange pas stjålet/tabt i kommunerne. I starten af 2016 berettede flere medier om tabte/stjålne danske pas.²⁴ Tabel 3.1 viser en oversigt. Rigspolitiet er blevet spurgt om antallet af stjålne/tabte pas i 2016, 2017 og 2018. Vi har modtaget tallene for 2016 og 2017. Historisk set bliver ca. 35.000 danske pas hvert år registreret som stjålne/tabte.

Tabel 3.1 Danske pas: udstedte og bortkomne (stjålne/tabte) i perioden 2010-2017

	Udstedte	Bortkomne (brutto)	Tilbage	Bortkomne (netto)
2010	680.694	38.043	10.263	27.780
2011	637.711	37.989	10.501	27.488
2012	634.628	36.363	9.955	26.408
2013	580.967	34.949	9.512	25.437
2014	584.209	35.149	9.386	25.763
2015	696.254	43.818	11.782	32.036
2016		35.521		
2017		34.634		

Kilde: Politiets pasregister

Et pas kan bruges til at krydse grænser under en falsk identitet eller til at misbruge den retmæssige ejers identitet. Hvor mange af de stjålne/tabte pas, der er blevet brugt til identitetsmisbrug, er ukendt.

Ifølge Transportvaneundersøgelsen (DTU Transport, 2014) har 88 % af danskerne over 18 år kørekort, og 83 % af danskerne har adgang til mindst én bil i husstanden. Derfor må vi antage, at langt de fleste danskere ofte har deres kørekort med sig – typisk i deres pung. Når de mister deres pung (taske), så mister de ofte også deres kørekort. Selvom kørekortet officielt ikke betragtes som legitimationsbevis, bliver kørekortet typisk brugt til at legitimere sig i alle

²³ NemID er en sikkerhedsløsning, der kan bruges til netbank, offentlige og private hjemmesider og digital signatur. En borger kan få NemID, når pågældende er fyldt 15 år, har et dansk cpr-nummer og kan opfylde legitimationskravene. NemID består af et bruger-id, en adgangskode og et nøglekort, der angiver de engangskoder (kaldet nøgler), som skal testes ind sammen med bruger-id og adgangskode. Det er ligeledes muligt at installere en NemID-nøgleapp på en mobilenhed og bruge den som nøgle.

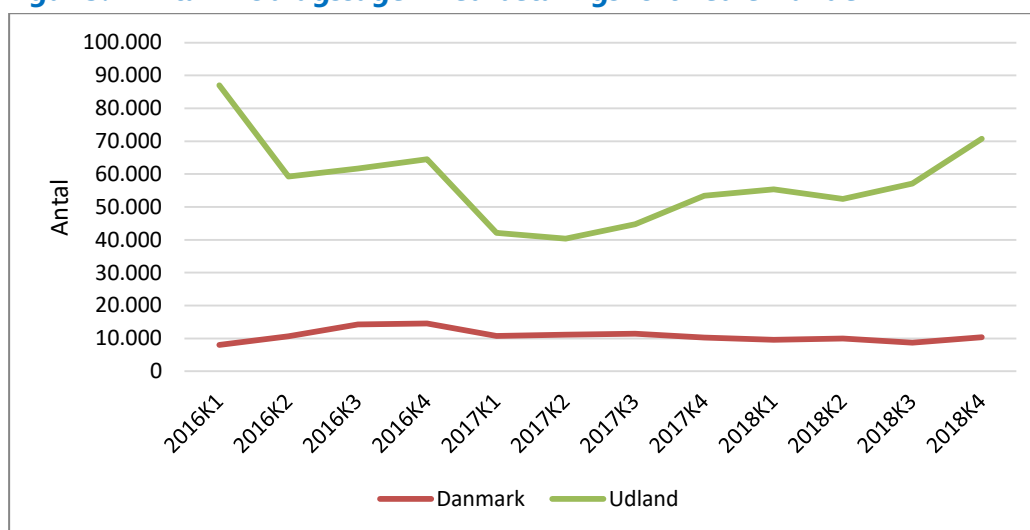
²⁴ Se fx <https://www.berlingske.dk/samfund/tusindvis-af-danske-pas-forsvinder-hvert-aar>

mulige sammenhænge. Rigspolitiet oplyser, at ca. 55.000 kørekort hvert år bliver meldt stjålet/tabt. Tallene for 2016, 2017 og 2018 er henholdsvis 53.878, 57.067 og 55.025.

Sundhedskortet – som mange danskere også har med sig i deres pung – bliver i offerundersøgelser (Kruize 2017 mm) nævnt som et identitetsbevis, der anvendes ved identitetsmisbrug. Vi har ikke indblik i, hvor ofte danskere har meldt deres sundhedskort tabt eller stjålet.

Endelig er der betalingskort, som er en slags identitetsbevis, der giver adgang til den pågældendes bankkonto. Det fysiske betalingskort kan være kommet i hænderne på misbrugeren, men oftere har vedkommende fået kendskab til kortets 16 cifre (på forsiden) og de 3 CVC-cifre (på bagsiden). Det er ikke altid nok at have kendskab til disse cifre for at købe på nettet. Visse steder spørges der om en form for validering (*Verified by* eller NemID-validering). Figur 3.1 viser, at misbrug af danske betalingskort for en stor dels vedkommende foregår på udenlandske e-handelsmarkeder. Antallet af misbrugssager faldt i 2017 i forhold til 2016, men 2016 lå også på et ekstremt højt niveau, historisk set (se Kruize, 2018, s. 42-44). I 2018 tog misbruget på udenlandske e-handelsmarkeder igen til.

Figur 3.1 Antal misbrugssager med betalingskort ved e-handel



Kilde: Nationalbankens Statistikbank

3.2 Metoder til at misbruge identitetsoplysninger (modus)

Det er svært at udarbejde en udtømmende liste over alle former for økonomisk identitetsmisbrug, men herunder omtales de mest hyppige former for misbrug:

1. Køb, lej eller leasing af varer i fysiske butikker
2. Køb af varer i webbutikker
3. Pengeoverførsel i netbanken

4. Oprettelse af et forbrugslån (kviklån)
5. Oprettelse af en virksomhed
6. Modtagelse af strandet besked og CEO-bedrageri
7. Handelsbedrageri
8. Datingbedrageri.

3.2.1 Køb, lej eller leasing af varer i fysiske butikker

Det er efterhånden i langt de fleste butikker sådan, at hvis man vil købe på kredit, skal man vise en form for billedlegitimation for at bekræfte ens identitet. Langt de fleste mennesker har altid deres kørekort på sig, og hvis en taske eller pung bliver stjålet, er der stor risiko for, at kørekortet dermed falder i tyvens hænder.

I en sag fra 2013 blev en kvindes pung stjålet, og efterfølgende blev hendes kørekort – med et falsk billede – misbrugt til en stor indkøbstur på kredit i ti butikker i løbet af 14 dage. I en af butikkerne blev gerningskvindens ansøgning til et lån afvist, men i de andre ni butikker blev der indkøbt for over 200.000 kr. i alt. I en af butikkerne var gerningskvindens ansigt synligt på overvågningsvideoen, og dermed kunne offeret selv finde frem til kvinden gennem en privat efterforskning på Facebook.

En anden mulighed, ifølge en politirespondent, er at ringe ind til butikken, Dermed undgås det, at et identitetsbevis skal fremvises.

Vi ser mange sager omkring, hvor de ringer ind og bestiller telefoner. Det kan man godt gøre telefonisk. Her skal man bruge cpr-nr., men ikke NemID. Herefter bliver telefonen sendt til en pakkepost, hvor gerningsmanden henter den, mens den forurettede kommer til at stå med abonnementet og regningen.

Et eksempel på leje af varer er en sag fra 2011. En mand fik stjålet sin pung med bl.a. sit kørekort og sygesikringsbevis. Ved hjælp af disse to identitetsbeviser lejede to gerningsmænd for 200.000 kr. musikudstyr i flere butikker uden at levere det tilbage. Også i denne sag blev kørekortet forfalsket, det vil sige, at der var indsat et andet billede.

3.2.2 Køb af varer i webbutikker

Køb af varer på kredit i en fysisk butik kræver, at man identificerer sig, typisk med legitimation med et billede på. Dette kræves ikke ved e-handel. For det meste købes varer over nettet ved betaling med et betalingskort. En del af denne handel foregår med stjalne betalingskort. Misbrug af betalingskort kan også kombineres med identitetsmisbrug. Interviewrespondenten fra Fyns Politi beskriver den metode på følgende måde.

Handlen på nettet med stjålne kreditkortoplysninger, så er det mit indtryk, at der ret ofte bliver misbrugt en anden persons identitet ved bestilling af varerne i webbutikker. Hvad der sker i stor stil er, at folks navne og bopælsadresser tages fra f.eks. Krak eller andre søgemaskiner, og så bruger man dem som bestiller. De bruger stjålne kortoplysninger, som hører til en anden person og et mobilnummer, der er tilknyttet et ikke-registreret taletidskort. De får en sms om, at der er leveret en pakke til pakkeboksen, hvorefter gerningsmanden kan afhente pakken ved boksen.

Der findes stadig webbutikker, hvor man kan købe på kredit ved hjælp af en persons cpr-nummer. I et interview i september 2017 med en repræsentant for Midt- og Vestjyllands Politi pegedes i denne forbindelse på Ellos.²⁵

Man skal give navn, adresse og cpr-nummer for at bestille varer hos Ellos. Når det er en ny kunde, så foretager de en kontrolopringning. Der er ingen af sagerne, der er gennemført. Ikke hvor jeg har kendskab til det. Kontrolopringning, hvor de spørger, har du bestilt det her. Hvis de siger nej, så sletter de ordren med det samme. Der er kun forsøg. Et par stykker hver uge. Det er et af de få steder, hvor man kan købe kun med cpr-nummer.

3.2.3 Pengeoverførsel i netbanken

Finans Danmark skelner mellem netbankindbrud og social engineering. Netbankindbrud omfatter sager, hvor der er sket indbrud eksempelvis ved installation af hacker-programmer på brugerens PC, mobil eller tablet, og fremgangsmåden kan være kombineret med bedrageri. Social engineering omfatter sager, hvor brugeren lokkes til at afgive eller indtaste oplysninger (id, password og nøglekortkoder) til gerningsmænd på baggrund af falske e-mails, SMS eller telefonopkald. Disse giver sig ud for at komme fra eksempelvis et velrenommeret selskab, en myndighed eller en ven.

Finans Danmark har siden 2006 ført statistik over netbankindbrud. I perioden 2006-2017 ser vi to gange et drastisk fald i antallet af netbankindbrud (se Figur 3.2). Den oplagte forklaring på det første fald (2010-2011) er introduktionen af NemID, Danmarks digitale signatur. NemID introduceredes 1. juli 2010 og anvendes til at få adgang til både netbank og offentlige services. Den afgørende forskel mellem NemID og den tidligere opkobling²⁶ til netbank er nøglekortet eller nøgleviseren. Hver gang, en kunde logger ind på sin netbank, kræves en unik, sekscifret nøgle, der aflæses på kortet/viseren. Dermed er der indlagt en væsentlig ekstra teknisk sikring. Figur 3.2 viser imidlertid også, at antallet af netbankindbrud allerede faldt til nul i det første halvår af 2010 – perioden umiddelbart før introduktionen af NemID. Den

²⁵ Ellos (www.ellos.dk) er mest kendt som tøjbutik, men sælger også varer i kategorierne 'bolig og indretning', 'skønhed' og 'elektronik'.

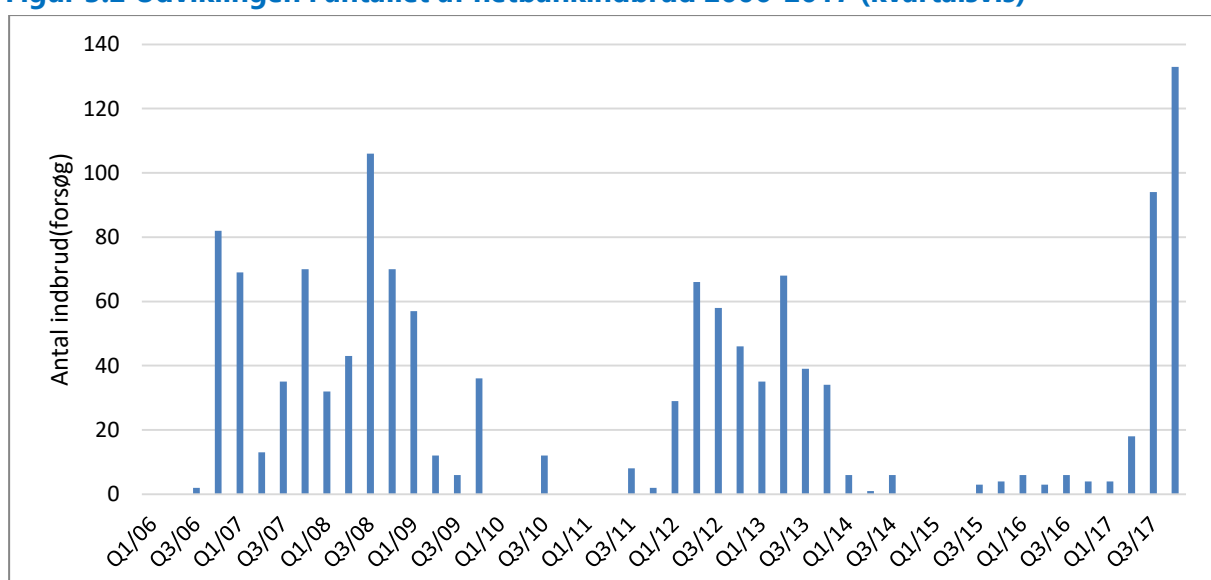
²⁶ Før introduktionen af NemID krævede adgang til netbank en logfil på computeren samt brugernavn og password. Adgang til computeren og afluring af id-oplysninger var således nok for it-kriminelle til at kunne begå netbankindbrud.

supplerende forklaring er, at nogle dataservere, som hackere brugte ret aktivt, blev lukket ned i løbet af 2009 (Kruize, 2018, s. 37).

Faldet siden 2014 forklares ikke med et kriminalpræventivt tiltag, men med en ændring i de kriminelles adfærd. På Finans Danmarks (dengang Finansrådets) hjemmeside gives følgende forklaring på 2014-faldet:

Vi ser lige nu en ændring i angrebsmønstret hos de it-kriminelle, og lige for tiden er de angreb, der rammer kunderne, ikke netbankindbrud. I stedet snydes kunderne til selv at gennemføre overførslerne eller sende deres nøglekort til de kriminelle. Desværre lykkes det ofte, og derfor er der god forretning for de kriminelle i denne meget enkle kriminalitet, hvor kunden blot spørges pænt om alle sikkerhedskoder, og et indbrud derfor ikke er nødvendigt.

Figur 3.2 Udviklingen i antallet af netbankindbrud 2006-2017 (kvartalsvis)



Kilde: Finans Danmark

Senere betegner Finans Danmark denne form for netbankkriminalitet som *social engineering* og har siden 2016 ført statistik over disse sager. I 2016 registreredes der næsten udelukkende social engineering-sager, men i 2017 vendte netbankindbrud tilbage. Forklaringen findes i de såkaldte bibliotekssager. I de her sager installeres keylogger-software på bibliotekets computere. En keylogger er et program, som opsnapper alle tastetryk og sender dem tilbage til en bagmand.

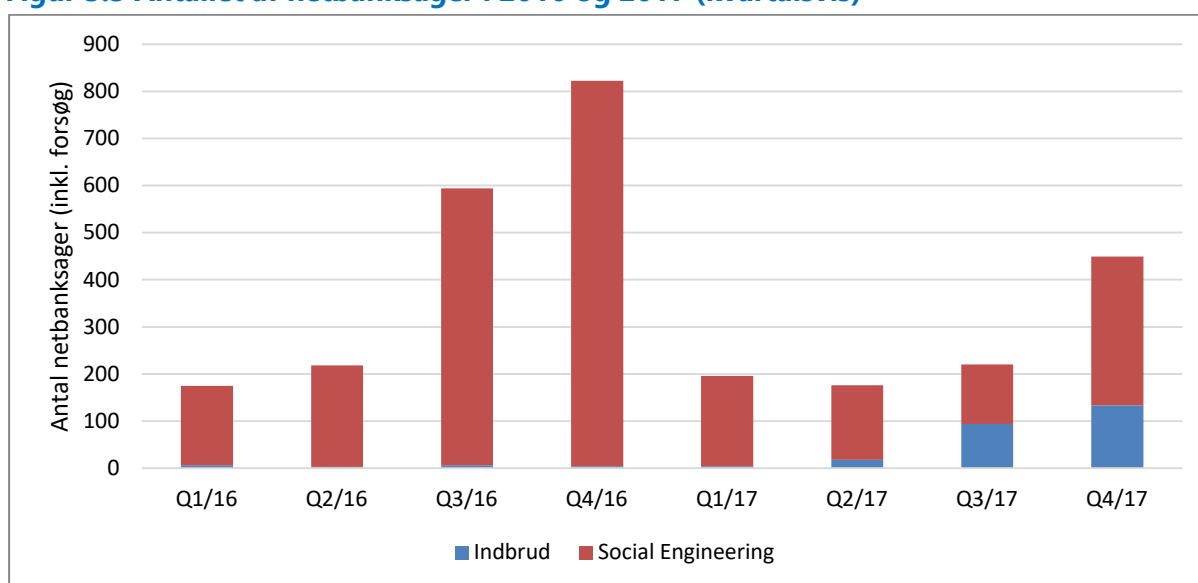
To mænd er blevet idømt tre og fem års fængsel for at have installeret Spyware på 15 biblioteker. De to mænd på 25 og 30 år havde installeret keyloggere på bibliotekernes computere fra sidst i 2016 indtil den 30. maj 2017, hvor de blev anholdt. Keylogger er et stykke software, der gemmer alle indtastninger på tastaturet. På den måde kunne de aflure personlige oplysninger og bl.a. få adgang til biblioteksbrugernes bankkonti og oprette lån og bestille kreditkort og

NemID-nøglekort. 16 danskere er blevet ofre for bedrageriet, og de to mænd har hævet og forsøgt at hæve for i alt otte millioner kroner.

<https://www.dr.dk/nyheder/regionale/syd/hackede-sig-til-otte-millioner-kroner-paa-bibliotekscomputere-nu-skal-broedre>

Det samlede tab ved pengeoverførsel i netbanken var i 2016 på 7,2 mio. kr. Dette beløb steg i 2017 til 11.0 mio. kr. Ca. halvdelen af 2017-tabet skyldtes netbankindbrud, mens den anden halvdel kunne tilskrives social engineering. Det gennemsnitlige tab ved netbankindbrud er ca. 30.000 kr., mens social engineering giver et gennemsnitligt tab på ca. 15.000 kr.

Figur 3.3 Antallet af netbanksager i 2016 og 2017 (kvartalsvis)



Kilde: Finans Danmark

3.2.4 Oprettelse af et forbrugslån (kviklån)

Der er mange butikker, hvor man kan få et lån til at købe varen. Det gælder f.eks. telecom- og elektronikbutikker, møbelforretninger og andre butikker, hvor mange køber forholdsvis dyre varer. Det er typisk en finansiel virksomhed, som står bag forbrugslånet. Der kan også optages et forbrugslån direkte hos en bank eller en udbyder af et såkaldt kviklån.

Ansøgning om et kviklån foregår typisk på nettet og kræver NemID-validering. Interviewrespondenterne i de enkelte politikredse tilkendegiver, at de ofte modtager anmeldelser om identitetsmisbrug, hvor gerningsmanden har optaget et kviklån. Ligesom ved netbankmisbrug kræver det adgang til offerets NemID-oplysninger, men ofte spørges også om årsopgørelsen og en lønseddel. Der er også kviklån-udbydere, som kræver samtykke til selv at hente årsopgørelsen hos Skat. Det har vist sig at være et ret effektivt præventivt tiltag, for så kan gerningsmanden ikke snyde med en falsk/forfalsket årsopgørelse. En politimand forklarer det således:

Når man opretter et forbrugslån, kan man give banken tilladelse til at hente din skattemappe. En anden mulighed er, at man selv går ind og tager kopier af ens lønsedler og årsopgørelser og sender det ind. Hvis man har rent mel i posen, mener jeg, at det er nemmere at sætte dét flueben. Det er Basisbank, som har indført, at man skal give samtykke til, at de må hente oplysninger fra din skattemappe. Så man har kun den mulighed. Det har nedbragt deres antal af bedragerisager betragteligt, fordi gerningsmændene går ud på gaden og presser sig til NemID'erne eller køber dem af folk, som oftest er unge mennesker. De har ikke en indkomst, der er høj nok, til at de kan få et lån på 100.000 kr. hos Basisbank. Derfor er det, at de bliver nødt til at indsende en falsk årsopgørelse.

Der findes ingen statistik for, hvor ofte der optages et kviklån ved identitetsmisbrug, men ud fra politiets meldinger samt udsagn af Basisbank – som tilbyder disse lån – findes der flere hundrede sager. Udbydere af kviklån er dog skeptiske over for, hvorvidt den person, der påstår, at hans/hendes identitet (NemID) er blevet misbrugt, er uvidende/uskyldig. Jeg vender tilbage hertil senere i rapporten.

3.2.5 Oprettelse af en virksomhed

I december 2014 handlede et afsnit af tv-udsendelsen Operation X (TV2) med titlen *De falske direktører* om svindel med virksomheder. Det er blevet nemt at oprette en virksomhed i Danmark. For en krone kan der oprettes et enkeltmandsfirma, og revision kan fravælges. I udsendelsen præsenteredes en mand, hvis identitet var blevet misbrugt til at oprette et firma i hans navn. Han anede intet, før virksomheden gik konkurs, og brevene fra Skat, regningerne og inkassotruslerne begyndte at vælte ind gennem brevsprækken. Der blev svindlet for 3 mio. kr. i hans navn.

I en anden sag fra januar 2015 blev en 18-årig gymnasieelev truet til at aflevere sine identitetspapirer. Et par måneder senere opdagede hans mor, at han var blevet indsat som direktør i et byggefirma. Formålet med firmaet var at svindle med moms.

Det er ukendt, i hvilket omfang virksomheder bliver oprettet med det formål at begå svindel og med uvidende personer indsat som direktører. Der kan online oprettes en virksomhed på www.cvr.dk. Det kræver NemID-validering at oprette en virksomhed. En af politirespondenterne giver udtryk for, at det ikke er et sjældent set fænomen, men om dem, hvis identitet bliver brugt hertil, kan betragtes som ofre, er tvivlsomt.

Det her med at blive indsat som en stråmand, som direktør i et firma – det ser vi i en del sager. Nogle af de her stråmænd er vel vidende om, at de får brugt deres identitet, mens andre ikke er vidende om det. Du kan være fra et østeuropæisk land, foregive du kommer til Danmark, få udleveret et dansk sygesikringsbevis og et NemID. Du behøver ikke engang at være i Danmark, du

kan blot sidde nede i Rumænien. På denne måde kan man binde sig som direktør i et firma herhjemme i Danmark. Det er en del af det europæiske fællesskab, arbejdsmarkedets frie bevægelighed. Vi har mange sager med SKAT, hvor vi kan se, at mange penge havner i nogle selskaber, hvor der er indsat en borger fra Rumænien.

3.2.6 Modtagelse af strandet besked og CEO-bedrageri

CEO-bedrageri retter sig mod virksomheder, mens en besked om, at man er strandet i udlandet, retter sig mod privatpersoner. Princippet i begge svindelnumre er det samme: Man prøver at lokke en medarbejder/ven til at overføre et pengebeløb. Et led i fupnummeret er, at gerningsmanden skriver i en anden persons navn. På den måde kan også disse former for bedrageri betragtes som en form for identitetsmisbrug.

Ved CEO-bedrageri sender gerningsmanden en e-mail til en (regnskabs)medarbejder i topchefens navn eller på dennes vegne. Det kan være, at topchefens e-mail er hacked, men der kan også benyttes en anden e-mailkonto. I e-mailen bedes (regnskabs)medarbejderen om at overføre et stort beløb til en eller flere banker i udlandet. Alt skal naturligvis holdes meget fortroligt, idet der er tale om en transaktion, som foreløbig skal holdes hemmelig. E-mailen kan blive fulgt op af flere e-mails eller telefonopringninger med det formål at stresse medarbejderen med korte deadlines. Varianter af denne form for bedrageri består i, at en svindler udgiver sig for at være en advokat, der har fuldmagt til at handle på vegne af topchefen.

I starten af 2016 meldte SØIK, at der har været to store CEO-bedragerisager. I den ene sag blev virksomheden snydt for 100 mio. kr., mens udbyttet lå på 40 mio. kr. i den anden sag. NC3 citeres i Trusselsvurdering af Center for Cybersikkerhed (februar 2017) for, at antallet af CEO-bedragerisager er vokset markant, og at de i anden halvdel af 2016 modtog anmeldelser for 180 mio. kr. Det er ikke kun private virksomheder, som har været udsat for denne form for bedrageri. Også offentlige institutioner er blevet taget ved næsen; Patent- og Varemærkestyrelsen blev bedraget for 6,7 mio. kr. i 2016, og Statens Museum for Kunst blev i vinteren 2017 snydt for godt 800.000 kr.

Ved en 'strandet i udlandet'-besked bliver der sendt en e-mail eller en anden besked (f.eks. på Facebook) til venner og/eller familie med en opfordring til at sende penge; typisk til Western Union. E-mailen er for det meste hacked, og dermed er e-mailadressen korrekt. Opfordringen til at sende penge er ofte skrevet på dårligt dansk, så ikke så mange hopper på det. En anden ting er, at email-kontoen bliver skiftet til et sprog, som de fleste danskere ikke magter. Dermed er det svært at rette op og få sin e-mailkonto, med kontaktoplysninger, tilbage. Denne form for bedrag var populær for nogle år siden og blusser engang imellem igen op. Lokalpolitiet i Skive advarede i maj 2017 om, at der blev sendt beskeder om, at folk var strandet i Ukraine.

Efter to nye tilfælde af bedrageriforsøg advarer lokalpolitiet i Skive mod forsøg på bedrageri, hvor folk foregiver at være strandet i udlandet og at have mistet både pas og penge. Typisk ligner det en e-mail fra en bekendt eller en ven, men det er altså bedrageri. I Skive har politiet fået to anmeldelser tirsdag – og i begge tilfælde skulle de pågældende være strandet i Ukraine.

<https://www.skivefolkeblad.dk/article/20170531/LOKALT/170539974>

3.2.7 Handelsbedrageri

Antallet af private handler over nettet vokser støt. Derved bliver man engang imellem snydt. For at være sikker på, at sælger (og køber) har rent mel i posen, bliver der i nogle handler udvekslet dokumentation. Det kan være en vej til identitetsmisbrug, hvis den modtagende part genbruger de tilsendte dokumenter til et fupnummer. I 2017 sendte DR3 en programserie under titlen *Mit liv er stjålet*. En af de personer, der optrådte i programmet, havde sat sin bil til salg. Han blev kontaktet af en person, der gerne ville se registreringsattesten og servicebogen. Sælgeren sendte en kopi. Efterfølgende blev bilen solgt til en anden person. Senere opdagede han, at hans gamle bil blev tilbudt til salg på bilbasen. Han kontaktede bilbasen, som fjernede annoncen, men den blev oprettet igen og igen.

Der er også eksempler på sager, hvor folk har sendt en kopi af et identitetsbevis og efterfølgende optræder som sælgere i annoncer på nettet. De personer, der tilbyder f.eks. en iPhone i deres navn, sender gerne en kopi af deres identitetsbevis for at virke troværdige, men sender aldrig varen efter modtagelse af betaling. Resultatet er, at de identitetsmisbrugsudsatte bliver hængt ud på nettet som bedragere og bliver kontaktet af bedrageriofre med krav om, at disse vil have deres penge tilbage.

3.2.8 Datingbedrageri

En persons (profil)billeder kan blive misbrugt for at genere velkommende – hvilket omtales i næste kapitel om ærekrænkende misbrug – men kan også misbruges med et økonomisk sigte. En specifik form for datingbedrageri er 'romance scams', som retter sig primært mod kvinder over 40 år. Nordsjællands Politi advarede i en pressemeddelelse mod denne form for bedrageri. Kvinden kommer i kontakt med en mand på et socialt medie eller på et datingsite. Manden sender romantiske beskeder og er generelt særdeles indsmigrende. Når samtalen har stået på i en længere periode – og der er opbygget et tillidsbånd – beder gerningsmanden om at få overført penge til en bankkonto; oftest under påskud af at skulle betale et sygehusophold, have indløst en særlig pakke eller noget helt tredje. Identitetsmisbrug kommer på tale, når en anden persons billeder bliver brugt til profilen. Radioværten Dan Rachlin har

oplevet mange gange, at hans billeder (med hans børn) bliver brugt igen og igen. I et interview med Ekstra Bladet (18. februar 2018)²⁷ sagde han:

Så sent som for 14 dage siden var der en kvinde i USA, som fortalte mig, at hun havde spenderet 65.000 dollars på en falsk profil, hvor manden med datteren fortalte, at datteren var hjertesyg og havde brug for en operation. Der bliver brugt mange penge på godtroende, primært midaldrende kvinders bekostning.

3.3 Offerprofil

I offerundersøgelserne Internetkriminalitet 2014 og 2017 (Kruize, 2015; 2018) tilkendegav i alt 105 personer, at de havde været udsat for identitetsmisbrug med et økonomisk sigte. Når disse personers profiler sammenlignes med den danske befolkning som helhed, er konklusionen, at identitetsmisbrug med økonomisk sigte rammer bredt. Der gælder såvel udsattes køn og alder som etnisk oprindelse, type af kommune og sammensætning af husholdningen.

Repræsentanter for centrale aktører er i interviewene blevet spurgt om, hvorvidt de kan tegne en profil af de personer, der bliver udsat for økonomisk identitetsmisbrug. Disse repræsentanter er delt op i tre grupper: politiet, kreditorerne og støtterne. Herunder redegøres for deres syn på offerprofilen.

3.3.1 Set med politiets øjne

Politiet ser, hvis sagen anmeldes, en bred vifte af former for økonomisk identitetsmisbrug. Interviewrespondenterne bekræfter også, at der findes mange former for misbrug, og politirespondenter tilkendegiver, at disse former for misbrug rammer forholdsvis bredt. Alle kan miste en pung med kørekort eller sundhedskort eller tabe deres betalingskortoplysninger pga. nethandel.

Der er den helt almindelige dansker, som bliver hacket eller taber sin pung. Lige pludselig begynder det at vælte ind med regninger på nettet. Vi ser ikke lige så ofte sager, hvor både sygesikringskort og kørekort er blevet misbrugt, men her kan de gentagne gange misbruge i vedkommendes navn. Misbrug af personoplysninger på nettet ser vi rigtigt meget af, også fordi man kan købe kreditkortoplysninger billigt på nettet. Det her er mere et bedrageriforhold end et tyveri af personlige oplysninger. Når vi er ovre i identitetstyveri, så er det mere noget med, at der bliver oprettet en masse ting i forskellige firmaer i ens navn. Der er en, som er gået ind og har overtaget en andens identitet.

²⁷ <https://ekstrabladet.dk/flash/dkkendte/frustreret-dan-rachlin-det-er-som-at-slaa-i-enedyne/7046183>

Men politirespondenter peger også på bestemte grupper, typisk når NemID-oplysninger er blevet (mis)brugt. De skelner overordnet mellem tre udsatte grupper, over for hvilke der anvendes forskellige fremgangsmåder:

1. Oplysninger franarres svage eller ældre borgere.
2. Oplysninger (mis)bruges af familie/bekendte.
3. Oplysninger afpresses/franarres i gademiljø.

Svage eller ældre borgere

Den første gruppe, som en del af politirespondenterne peger på, er svage eller ældre borgere. De er godtroende eller uvidende om, hvad der foregår, når de franarres deres oplysninger. Interviewrespondenter beskriver det, som følger:

Vi har en del sager, hvor folk på den ene måde måske er lidt naive, men også nogle, som bare er lidt svage. De udleverer simpelthen deres NemID, fordi de tror på den løgnehistorie, som de kriminelle gerningsmænd kommer med.

Gerningsmændene går også efter beboere på bosteder og handicappede, som ikke er så dårlige, at de ikke kan have et NemID. Hvis en beboer fra et bosted får en rykker, gør de ikke så meget ved det. Nogle af dem kan jo ikke engang læse. Det tager ofte noget tid, inden vi får anmeldelserne fra de her situationer. Det er nogle rigtige lortesager.

Det kan også være mere svage borgere. Mange af dem er myndige, de er i hvert fald ikke umyndiggjort, selvom de måske har forskellige svagheder. Så er de i stand til at klare sig selv, og de bliver narret i et vist omfang. Når kriminelle har deres fingre i NemID-oplysninger, så opretter de typisk et kviklån eller et benzinkort eller bestiller tøj på nettet med levering til pakkeboksen.

Familie eller bekendte

Misbrug af familie eller bekendte kan faktisk også ramme bredt i befolkningen. Kendetegnende er her, at udsatte og gerningsmanden er eller har været tæt på hinanden, og at det dermed er relativt nemt at få fat i udsattes NemID-oplysninger. En af politirespondenterne bemærker i denne sammenhæng, at man burde holde sine personlige koder hemmelige, også i et parforhold. Det lyder som en god idé, men strider samtidig mod grundlaget, hvorpå et kæresteforhold er bygget: tillid til hinanden.

Vi har nogle sager, hvor man mistænker en ekskæreste for at have brugt personlige oplysninger. Her kan være nogle reelle tilfælde. Jeg tror dog ofte, det er planlagt mellem den forurettede og gerningspersonen. Sommetider er det også inden for familier internt. Det er måske sønnen, som køber noget i forældrenes navn.

Gademiljø

Specielt politirespondenterne i og omkring København beretter om folk, der afpresser unge til at afgive deres NemID-oplysninger eller bliver lokket hertil for at tjene nogle lette penge. Der henvises til hash-miljøet. Der berettes om, at det kan være ret organiseret med forgreninger til udlandet. Herunder ses et udpluk fra to af interviewreferaterne.

Det, vi oplever her lokalt os hos, er, at vi mener, der er nogle bagmænd. Vi har også nogle reelle sager, hvor vi går efter bagmændene. De arbejder med det her. De har folk under sig. De har folk til at skaffe NemID'er; enten ved at købe det eller presse sig til det. Med NemID'erne optager de en masse lån, pengene bliver overført. Det er meget organiseret. De udsatte får penge for at udlevere deres NemID. Det handler om grådighed. Der er to slags hælere. Der er dem, som selv stiller deres konto til rådighed. For det er klart, at de kan sløre pengesporet, hvis det går igennem fire konti, inden det ender hos den reelle modtager. Så får de 1000 kr. hver for at føre de her 40.000 kr. igennem. Her er det ikke NemID, som bliver misbrugt. De stiller deres konto til rådighed. Og så er der dem, som får stjålet eller misbrugt deres NemID. Gerningsmændene henvender sig til personer, som de mener, er villige til at sælge deres NemID.

Det er jo ikke en diskussion, om man selv har bragt sig i situationen eller ej, fordi hvis man anmelder, at ens identitet er blevet misbrugt, så er det jo klart, at vi optager en anmeldelse. Vi er objektive i vores efterforskning. Vi skriver selvfølgelig ned, hvis den forurettede selv fortæller at have udleveret sit NemID. Så er det jo klart, at vi skriver det ned i rapporten. Politiets fornemste opgave er at belyse sagen objektivt, men man kan ikke altid lade være med at spørge ind til, hvorfor der blev udleveret NemID til at starte med. Vi går derfor meget tæt på at spørge ind til sagen. Den skal belyses ordentligt. Så kan den forurettede måske svare, at han blev afpresset, eller at han stolede på personen.

Forskellen mellem udplukkene fra det første og det andet interviewreferat er, at politiet i den første beretning ofte ser dem, der anmelder misbruget af deres NemID-oplysninger, som medskyldige, mens det ikke står til diskussion i den anden beretning. Den første beretning kommer fra Københavns Politi, og de melder også, at deres taktik nu er at prøve at få alle med. Det vil sige, at de også går efter de små hælerisager (dem, der har stillet deres NemID til rådighed, og/eller dem, der har stillet deres konto til rådighed). Bagmændene bliver dog første prioritet.

Hvæpsebosagen

Den såkaldte Hvæpsebosag handler bl.a. også om misbrug af identitetsoplysninger og viser, hvor organiseret identitetsmisbrug kan være. I 2015 ransagede politiet 62 adresser på Sjælland og Lolland-Falster og anholdt i alt 95 mennesker. Størstedelen af de anholdte var ifølge politiet ofre, men en gruppe rumænere, et par syrere og danskere blev retsforfulgt. Ifølge politiet er op mod 300 rumænere blevet opsøgt i Rumænien af landsmænd og lokket med en bedre fremtid og arbejde i Danmark. De blev transporteret til Danmark, hvor de blev huset og registreret og dermed fik NemID og cpr-nummer. Efterfølgende tog bagmændene rumæner-

nes danske identitetspapirer og brugte deres identiteter til bedrageri af særlig grov beskaffenhed. Samlet set mener anklagemyndigheden, at der blev svindlet for cirka 35-40 millioner kroner.

3.3.2 Set med kreditorernes øjne

Misbrug af betalingskort og cpr-nummer er fænomener, som alle danskere kan blive udsat for. Når det handler om misbrug af NemID-oplysninger, er billedet anderledes. At købe på kredit eller at optage et forbrugs- eller kviklån kræver nu til dags som regel NemID-validering. Når en person påstår, at hans eller hendes NemID-oplysninger er blevet misbrugt, har man i kreditorernes øjne været naiv, uagtsom eller medvirkende til misbruget. Det er forskelligt, hvordan kreditorerne reagerer i disse tilfælde. Hertil vender jeg tilbage i afsnittet om hæftelse.

De fleste interviewrespondenter, som repræsenterer kreditorerne, kan eller vil ikke skitsere en offerprofil. Undtagelsen er en respondent fra en bank, som har kørt mange NemID-sager i fogedretten. Hans beskrivelse stemmer til dels overens med politiets observationer. Også han genkender familie og kærester, der misbruger personernes oplysninger.

Der er mange ægtefæller, ekskærester eller andre familiemedlemmer, som sammen snyder. De problemer har vi altid haft, også før NemID. Der er flere kvinder end mænd, som gør det her. Vi har sågar haft kvinder, der ringede ind og talte med en mandsstemme, hvor vores medarbejder har sagt, at han godt kunne høre, at hun ikke var en mand, og så blev røret smækket på. Det mærkeligste eksempel, vi har haft, er for 7-8 år siden. Vi havde en mand, som ikke betalte sine lån, og vi hev ham i fogedretten. Konen mødte op med en fuldmagt med videre, så gik der 6 år, før manden ringer og siger, at han lige er blevet skilt, hvad er det her? Han har slet ikke anet noget om, hvad konen har foretaget sig. Han har stået i RKI uden at vide det.

Forleden havde vi en sag i fogedretten, hvor pengene ikke var overført til en NemKonto, men en anden konto. Her ringede de til selskabet, og de kunne fortælle, hvem som ejede kontoen. Det var mandens søn. Manden kunne så vælge at politianmelde sønnen, men det valgte han ikke at gøre. Han valgte, sammen med sønnen, at betale for lånet.

Også sager, hvor ofrene er svage eller demente ældre, genkendes af bankrespondenten. De er umyndiggjort, men det er ikke blevet tinglyst, at de er umyndiggjort. Det vil sige, at de kan optage et lån, og de penge får banken ikke tilbage, medmindre der findes frem til gerningsmanden.

Til sidst er der dem, der sælger deres NemID-oplysninger. Modsat politirespondenterne mener bankrespondenten ikke, at det ofte handler om udsatte unge.

Det, der undrer mig, er, at det ofte er folk i slutningen af 20'erne og starten af 30'erne med gode jobs, som udlåner deres NemID for at tjene småpenge. Det kan jeg simpelthen ikke forstå. Vi har haft nogle, som ikke kan forstå, at de har gjort noget galt. De kan ikke se, at det er bedrageri. Det er jo ikke dem, som har taget lånet, siger de. De er ikke engang ressourcesvage og skulle bruge pengene, men det kan vi ikke se, at det er. De er naive. Hvorfor er der så mange, som er så naive? Og hvordan kan det blive ved?

Respondenten fra en inkassovirksomhed mener, at dem, der har været udsat for identitetsmisbrug, har ordnet sagen, før den ender hos en inkassovirksomhed. I de få sager, han ser, kan dem, der hævder, at deres identitet er blevet misbrugt, betragtes som udsatte og er ofte blevet tvunget til at afgive deres identitetsoplysninger.

3.3.3 Set med hjælpernes øjne

En interviewrespondent fra Den Sociale Retshjælp fortæller, at de bistår 50 til 100 personer om året i forbindelse med identitetsmisbrug. Ca. tre ud af fire af disse sager relateres til, hvad hun betegner som et gademiljø.

De er presset til det. Hvis de ikke giver de oplysninger, så får de tæv. Så det er afpresning. Og vi kan ikke rigtigt gøre noget ved det. Så skal man bevise, at man er presset. Det kræver, at man stikker den, der har presset en, og det gør man ikke i det her miljø. Så får man bare endnu mere tæv, ikke? Vi kan fortælle om deres retsstilling og eventuelt en afdragsordning. Og så siger de for det meste, at det er lige meget. Det er mere på teoretisk plan. De kan heller ikke betale den gæld, der er stiftet i deres navn. Slet ikke. De er på kontanthjælp.

Men misbrug sker også i parforhold eller mellem bekendte, ifølge respondenten fra Den Sociale Retshjælp. Hun giver et eksempel på en konkret sag, som stemmer overens med det billede, bankrespondenten har tegnet, for så vidt de faktuelle oplysninger. Synsvinklen er dog ret anderledes set fra kreditorernes eller debitorernes side.

Sagen handler om en pige på 19 år, som havde det rigtig svært. Hun er droppet ud af skolen, lider af anoreksi og er psykisk hårdt ramt. Så kommer der en kammerat, som siger, at han gerne vil hjælpe hende. Der er nogle regninger, der skal betales. Han vil låne hendes bankoplysninger, for han vil overføre penge på hendes konto, for han er på kontanthjælp og laver sort arbejde engang imellem. Og det siger hun ja til, for hun stoler på ham. De har kendt hinanden i mange år. Og så pludselig begynder der at komme regninger ind ad døren. Bl.a. afdrag på et lån. Der er tre kreditorer, og så ringer hun til de tre kreditorer og spørger om, hvad er det her for noget, og så fortæller de hende, at hun har stiftet gæld. Så siger hun, at det har hun ikke og aldrig haft det arbejde, som står i deres register. De siger, der er ikke så meget at gøre. De siger, at hun må gå til sin advokat. Så kommer hun her. Og jeg kontakter kreditorerne, men de er ligeglade. Fordi der står ingen steder i loven, at kreditorerne skal dobbelttjekke de oplysninger, der bliver afgivet, man underskriver på nettet på tro og love og med sin NemID, og så går de ud fra, at alt er,

som det skal være. Derfor taber vi sagen i fogedretten. Der er ingen steder i lovgivningen, der siger, at de her lån kan omgøres.

Ligesom Den Sociale Retshjælp kan forsikringsselskaber hjælpe identitetsmisbrugsudsatte. Dem, der henvender sig til forsikringsselskaber, adskiller sig dog ret meget fra dem, der søger hjælp hos Den Sociale Retshjælp. Det er mere den 'gennemsnitlige' dansker, der gennem sin familieforsikring søger hjælp hos forsikringsselskaber. Ifølge Affinion, som bistår identitetsmisbrugsudsatte på vegne af deres forsikringsselskab, er de fleste af de udsatte, de bistår, i 20'erne.

4 Ærekrænkende misbrug

Ifølge offerundersøgelsen Internetkriminalitet 2017 (Kruize, 2018) er formålet med identitetsmisbrug for det meste at opnå en økonomisk gevinst. Der er dog et stigende antal sager, hvor der er tale om, hvad vi kalder ærekrænkende identitetsmisbrug (se også Figur 1.1). Dette begreb favner bredt. Det kan være tale om en bevidst strategi for at krænke en bestemt persons omdømme, men der kan også være tale om drilleri, drengestreger. Ærekrænkelse er et svært begreb, forstået på den måde, at det kan være svært at definere, hvilke handlinger der virker krænkende, for hvad der er krænkende for den ene person kan opfattes som ikke-krænkende af en anden person.

Oprettelse af en falsk profil på internettet, altså tilfælde, hvor man udgiver sig for at være en anden, kan som udgangspunkt ikke i sig selv betragtes som strafbart. Mobning eller chikane er heller ikke altid strafbart. Anklagemyndigheden har udgivet en pjece med råd og vejledning for dem, der er udsat for forfølgelse, chikane eller såkaldt stalking. Det anerkendes, at henvendelser, der ikke i sig selv er strafbare, kan opleves som ubehagelige og forstyrrende. Den konkrete vurdering af, hvorvidt der er tale om strafbar chikane, ligger hos politiet. På politiets hjemmeside kan man læse, at en række af bestemmelserne i straffelovens kapitel 27 om freds- og ærekrænkelser også gælder, når chikane eller lignende sker på internettet. Disse bestemmelser er imidlertid, med enkelte undtagelser, undergivet privat påtale; det vil sige, at det er op til den, chikanen retter sig imod, at anlægge en civil sag vedrørende spørgsmålet.²⁸

Privat påtale kan ske med henvisning til persondataloven. Det er derimod mere oplagt at rette henvendelse til Datatilsynet. Ifølge persondataloven kan man protestere mod offentliggørelse af oplysninger og/eller billeder, men kun hvis indehaveren ikke selv har lagt dem ud på internettet. Datatilsynet skriver i denne forbindelse: "Når du offentliggør billeder af eller oplysninger om dig selv, gør du det samtidig muligt for andre at bruge oplysningerne. Datatilsynet vil som oftest ikke kunne hjælpe dig med at få andre til at slette de oplysninger eller

²⁸ I en sag fra 2017 afviste politiet at hjælpe en kvinde, hvis profilfoto blev brugt til flere falske datingprofiler. Da hun ringede til politiet for at få hjælp, fik hun at vide, at politiet ikke kunne hjælpe hende, fordi billedet var kopieret fra hendes åbne profil på Facebook, og at det dermed var blevet allemands-eje. I Jyllands-Posten kritiserede Forbrugerrådet Tænk og Rådet for Digital Sikkerhed denne afvisning, men politiet holdt fast i sin vurdering. En talsmand fra politiet tilføjede: "Vi kunne godt have modtaget anmeldelsen og undersøgt sagen, men vi ville være kommet frem til den samme konklusion. Nemlig, at der ikke er nogen overtrædelse i det, og at hun selv måtte tage fat i en advokat og køre sagen selv som et civilt søgsmål".

billeder, som du selv har offentliggjort. Du kan eventuelt påberåbe dig ophavsret til dine billeder – men Datatilsynet kan ikke hjælpe dig med spørgsmål om ophavsret”.

I dette kapitel ser vi nærmere på de følgende former for ærekrænkende identitetsmisbrug:

- Overtagelse af udsattes profil eller konto (afsnit 4.1)
- Oprettelse af en profil/konto med udsattes oplysninger (afsnit 4.2)
- Uønsket deling og/eller manipulering af billeder/videoer (afsnit 4.3).

Kapitlet afsluttes med et afsnit om, hvem der typisk bliver udsat for ærekrænkende former for identitetsmisbrug (afsnit 4.4).

4.1 Overtagelse af udsattes profil eller konto

Når chikane består i uberettiget adgang til andres e-mailkonto, Facebook-profil eller lignende, kan straffelovens § 263, stk. 2, anvendes. Denne paragraf hører under straffelovens kapitel 27 om freds- og ærekrænkelser og er kendt som hacking-paragraffen:

§ 263, stk. 2 Den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem, straffes med bøde eller fængsel i indtil 1 år og 6 måneder.

Uønskede ændringer af en persons profil på et socialt medie blev for nogle år siden i pressen døbt *Face rape*. Politiken²⁹ berettede i 2013 om en sag, hvori to teenagedrenge ved retten i Helsingør idømtes bøder på henholdsvis 2.000 og 4.000 kr. for at logge ind på en jævnaldrende piges Facebook-konto og ændre hendes profil. Drengene sigtedes for overtrædelse af brevhemmeligheden, blufærdighedskrænkelser og for at viderebringe meddelelser om andres forhold.

På Red Barnets hjemmeside bliver *Face rape* beskrevet, som følger:

Et *Face rape* betyder kort sagt, at man skaffer sig adgang til en anden persons profil på et socialt medie og ændrer profilens billeder eller skriver nye kommentarer eller tekster. Ordet 'Face rape' er en sammensætning af navnet på det sociale medie Facebook og det engelske ord for voldtægt: 'rape'. Ofte bliver *Face rapes* udført, hvis man eksempelvis går fra sin tændte computer, mens man er logget ind på et socialt medie. Eller hvis lægger sin mobiltelefon fra sig, og andre kan få adgang uden kode. Et *Face rape* kan være uskyldigt drilleri mellem venner – men det kan også være en ondsindet handling, hvor målet er at ydmyge den anden bruger. Selvom et *Face rape* kan være ment for sjov – og selvom *Face rapes* er ret udbredte – er det vigtigt at huske på,

²⁹ "Drenge får bøde for at ændre i piges Facebook profil", Politiken, 20. februar 2013.

at Face rapes handler om, at man skaffer adgang til andres private informationer, uden man har fået lov. Udøvere af Face rapes kan i teorien blive sigtet for hacking med fængselsstraf til følge.

De seneste år tales om hijacking eller hacking. Der har været indberetninger om hacking af profiler på adskillige sociale medier. Formålet med at hacke sig ind på en anden persons profil kan være forskelligt. Når det er bekendte, der står bag hacket, så er det typisk for at drille eller for at mobbe personen. Hvis profilen er hacket af en ukendt person – måske fra udlandet – ligger der formentlig et økonomisk motiv bag hackingen.³⁰

Lene Wachter Lentz kritiserede i en kronik i Information (1. november 2018) den danske hacking-paragraf for at være alt for bred.³¹ Bestemmelsen omfatter også situationer, hvor der ikke er brudt en sikkerhedsforanstaltning. Hun illustrerede sin pointe med en dom fra byretten, stadfæstet i landsretten, som handlede om en kvinde, der havde skaffet sig uberettiget adgang til sin ekskærestes Facebook-profil. Kvinden forklarede, at han havde givet hende passwordet til sin profil, og at hun havde fundet ud af, at han havde været hende utro. Hun benyttede derfor adgangen til hans profil til at drille ham ved at ændre brugernavn, adgangskode og profilbillede. Hun forklarede, at det er helt almindeligt at ændre andres profiler på Facebook, f.eks. hvis en person ikke er logget af, og at det ikke ville tage nogen tid at genoprette en ændret konto. I byretten blev kvinden idømt 20 dagbøder a 100 kroner. Anklagemyndigheden ankede til landsretten for at få en fængselsstraf, men landsretten var enig i bødestraffen. Lene Wachter Lentz konkluderede, at "det bør overvejes at begrænse strafansvaret til at gælde i de situationer, hvor offeret har beskyttet sine data med en sikkerhedsforanstaltning, som gerningsmanden har brudt. Dermed kan vi sikre, at meget drilleri, nid og nag mellem venner og bekendte på de sociale medier ikke bliver straffesystemets problem, men noget, man selv må løse".

4.2 Oprettelse af en profil/konto med udsattes oplysninger

Som beskrevet i indledningen til dette kapitel er det i sig selv ikke strafbart i Danmark at oprette en profil eller konto i et andet navn. Mange mennesker kan have det samme navn, og en falsk profil peger først på en bestemt person, hvis der tilføjes specifikke oplysninger

³⁰ En undersøgelse af Ultra Nyt (DR) i samarbejde med Epinion viser, at hvert fjerde barn i alderen 9 til 12 år har prøvet, at fremmede har sendt links, beskeder eller billeder fra deres konto, fordi den er blevet overtaget. Sanne Lind (Børnetelefonen) citeres af DR for følgende kommentar: "Vi får rigtig mange henvendelser fra børn, der er kede af det og oplever, at der har været nogle inde og skrive fra deres profil. Når børnene skriver med nogle fremmede på nettet, opstår utrygheden pludselig. Hvad nu, hvis mine billeder og beskeder pludselig bliver delt og vist frem?"

<https://www.dr.dk/nyheder/indland/en-russer-overtog-theodors-profil-det-var-virkelig-ubehageligt>

³¹ https://www.information.dk/debat/2018/10/kan-virkelig-vaere-rigtigt-facerape-vaere-strafbart?lst_cntrb

og/eller billeder. Når det er klart, at profilen lægger op til at være en bestemt person, men personen ikke selv står bag oprettelsen, så kan der være tale om overtrædelse af straffelovens § 264 d – også kendt som værn mod krænkelse af privatlivets fred. Ordlyden her er følgende:

§ 264 d Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget videregiver meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget en bredere offentlighed. Bestemmelsen finder også anvendelse, hvor meddelelsen eller billedet vedrører en afdød person.

Stk. 2. Foreligger der under hensyn til oplysningernes eller videregivelsens karakter og omfang eller antallet af berørte personer særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 3 år.

Ifølge straffelovens § 275 er forbrydelserne i dette kapitel (om freds- og ærekrænkelser), bortset fra §§ 266-266 b, undergivet privat påtale. Ifølge stykke 2 af § 275 kan der være tale om offentlig påtale efter forurettedes anmodning dertil i sager om overtrædelse af §§ 263-264 d og § 267, jf. § 268. Det betyder, at sager om privatlivets fred er underlagt privat påtale, medmindre anklagemyndigheden – efter forurettedes opfordring – vil tage sig af sagen. Vi vender tilbage til dette spørgsmål i kapitel 6.

Oprettelse af en profil eller en konto med andres oplysninger kan variere ret meget i alvorlighedsgrad. Det første eksempel stammer fra en pige, hvis billeder er blevet brugt til at skabe et andet omdømme af hende, end hun ønsker, men i interviewet giver hun udtryk for, at hun ikke er slået ud af det og tager det stille og roligt.

Jeg har op til flere gange oplevet, at mine billeder er blevet misbrugt på forskellige sociale medier. Det har bl.a. været på Ask, Instagram og Facebook. Misbrugerne lægger ordene i min mund. Jeg er en meget tynd og fit pige og deler ofte mine ferie- og træningsbilleder. Billederne bliver ofte misbrugt ved at udstille mig anderledes, end jeg ønsker. De skriver bl.a., at jeg bare elsker mig selv. Jeg tror, at det er piger, som kender mig, der lægger de falske profiler op. Det er ikke, fordi jeg decideret har fjender overhovedet. Folk kan jo elske en, og de kan hade en, og de kan skrive om en, hvad de vil. Jeg er ret sikker på, at den falske profil på Ask er lavet af en, som jeg kender.

I det næste eksempel har misbruget af billeder fået meget større konsekvenser for det pågældende offer. Han bliver hængt ud som pædofil på nettet. Moren ville ikke slette opslaget, efter at han havde kontaktet hende og havde prøvet at forklare, at hans billede var blevet misbrugt af nogen. Politiet ville ikke tage sig af sagen.

Det startede i februar 2014 med, at min gamle folkeskoleveninde tog kontakt til mig, fordi hun syntes, at der var et billede, hun kunne genkende af mig. Hun sender så linket til mig. Jeg kunne så se, at der var en bruger, der advarede mod denne profil af en mand, hvis billede var mit. Billedet er fra, da jeg var 17 år. Så der er åbenbart en mand, som har stjålet et af mine billeder og har brugt det til en falsk profil. Igennem denne her profil har han spurgt ind til mindreåriges sexliv. Moren advarer højt og bredt om denne her profil. Hun har taget et screenshot med et billede af mig, hvor hun skriver, at denne mand er pædofil. Og advarer alle mod mig.

Billeder bliver bl.a. brugt til at oprette en profil på en datingsite eller platform. Lige for tiden er Tinder et populært medie blandt det yngre publikum. Tinder markedsfører app'en med slagordene *Swipe. Match. Chat. Date*. Man opretter en profil og bliver efterfølgende præsenteret for andre brugeres profilbillede. Ved at swipe til højre synes man godt om nogen, ved at swipe til venstre bliver den anden ignoreret. Hvis begge personer synes godt om hinanden, er der et match.

I en sag fra 2015 blev en universitetslærers navn og billede brugt til at oprette en Tinder-profil. Først efter at en kvindelig studerende havde gjort ham opmærksom på profilen, fandt han ud af, at hans oplysninger blev misbrugt, og at flere af hans studerende var bekendt med profilen. I vores interview med ham spekulerer han over, hvorfor gerningsmanden har oprettet en profil med hans billede; hvad får han ud af det?

Jeg tror ikke, der er et personligt motiv bag det her. Jeg tror ikke, det er et menneske, som kender mig. Jeg tror, det er en helt tilfældig udvælgelse af mine billeder og oplysninger, der har fundet sted. Og så har den eller dem, som har stået bag profilen, matchet alle dem, de kunne komme til på Tinder-profilen. Blandt nogle af dem, som der blev matchet med, var nogle af mine studerende. Jeg har ikke nogen idé om, hvem der står bag profilen. Måske det er en fra Københavnsområdet, men jeg ved det ikke. Jeg har heller ingen idé om alderen på personen. Det, der er med det her set-up, er, at personen, som står bag, aldrig ville kunne mødes med nogen af de her kvinder, eftersom det er mit billede, der bliver brugt. Det ville aldrig kunne udmønte sig i noget fysisk møde. Det ville være en absurd ting at forestille sig. Vedkommende har sikkert fået et kick ud af det.

Det næste eksempel handler om en sag, hvori formålet med oprettelse af en Facebook-profil i udsattes navn må have været hævn. I denne sag bliver der også aktivt søgt kontakt med arbejdskolleger, formentlig for at sprede de falske opslag til en større personkreds.

C. W. oplevede for et par år siden, at en person oprettede en profil på Facebook i hendes navn med hendes billede og hendes oplysninger. Den falske C. W. blev venner med den ægte C. W.'s kolleger på det sociale medie og begyndte at lave personlige og intime statusopdateringer som "Er lidt nede, har lige skændtes med kæresten" og "Er på vej i bad, trænger til at blive barberet". Først da kollegerne kom med bemærkninger om, at hun var på Facebook, blev hun opmærksom på det. Billedet og oplysningerne lå på nettet og kunne findes via hendes firmahjemmeside, ar-

tikler og blogs. Hun er ikke 100 % sikker på, hvem der gjorde det. Men hun tror, at det er en person, der var ude på at genere hendes mand.

I det sidste eksempel på oprettelse af en profil i udsattes navn optræder hævnmotivet igen, men her optræder gerningskvinden chikanen yderligere ved at dele udsattes telefonnummer og opdigtede sexydelser.

Klokken var lidt over seks en mandag aften, og C. stod og lavede mad sammen med sine børn, da hendes arbejdstelefon pludselig ringede. I røret fik hun en mandsperson, der med indsmigrende stemme forklarede, at han gerne ville dyrke bizar sex med hende. C. afviste uforstående manden, men hendes undren nåede ikke at bundfælde sig, før den næste sexvillige mand ringede. Telefonstormen ville ingen ende tage, og hun kunne høre, hvordan opkaldene stod i kø, mens hun afviste den ene mand efter den anden. Til sidst måtte hun slukke sin arbejdstelefon for at slippe for de sexhungrende mænd.

Det viste sig senere, at en kvinde, som hun var uvenner med, havde oprettet to datingprofiler i hendes navn. Datingprofiler, hvor hun tilbød en lang række sexydelser. Ikke blot almindelig sex, men også en lang række af bizarre former for sex. Hendes telefonnummer og e-mailadresse stod i datingprofilerne, ligesom hendes mest kendte fotografi prydede profilerne.

4.3 Uønsket deling og/eller manipulering af billeder/videoer

Den sidste form for ærekrænkende identitetsmisbrug, vi omtaler i dette kapitel, er uønsket deling – eller manipulering – af billeder eller videoer. En del sager, der hører til under denne overskrift, bliver ofte kaldt hævnporno. Red Barnet beskriver hævnporno således på sin hjemmeside:

Når andre offentliggør nøgenbilleder af andre på nettet, kaldes det hævnporno. Det kan for eksempel være en ekskæreste, der har fået tilsendt sådanne billeder i en privat sammenhæng, og som så vælger at lægge billeder ud til andre bekendte for at få ram på ekskæresten. Hævnporno er en grov krænkelse af den, det går ud over, og kan have alvorlige konsekvenser for offeret.

I Red Barnets beskrivelse bliver hævn eksplicit nævnt som motiv, og også i pressen bliver deling af nøgenbilleder hurtigt døbt hævnporno. Men der kan selvfølgelig også være andre motiver til, hvorfor nøgenbilleder eller sexvideoer bliver delt. Dansk Stalking Center påpeger på sin hjemmeside, at der ofte skelnes mellem hævnporno og pornografi uden samtykke, da motiverne til handlingerne kan være forskellige. Begge begreber refererer dog til deling af seksuelle billeder, nøgenbilleder eller videoer af en person, uden personens samtykke. Ofte er hævnpornobilleder taget af de udsatte selv. Ifølge Levendowski (2014) er 80 % af alle hævnpornobilleder selfies, som typisk er blevet delt med en tidligere kæreste. Ifølge Dansk Stalking Center er offentliggørelse af den udsattes navn, bopæl, alder, mobilnummer samt links til online sociale profiler ofte en del af hævnpornoen.

Umbrella-sag

Den mest kendte sag i Danmark om ulovlig deling af en sexvideo er uden tvivl Umbrella-sagen. Sagen startede i marts 2015 og handlede om en 15-årig folkeskolepige fra Nordsjælland, der havde sex med en ven. Senere kom fire af drengens venner forbi, og pigen blev udsat for overgreb, og der blev optaget tre videosekvenser af hende, mens hun havde sex med en af drengene.³² En uge senere begyndte optagelserne at florere på de sociale medier, og et år senere (marts 2016) blev to drenge idømt bøder på 2.000 kroner for at have delt børneporno. Videoerne fortsatte dog med at blive spredt på nettet. Facebook meldte sagen til de amerikanske myndigheder med oplysninger om mere end 5.000 delinger af videoerne på Messenger. De amerikanske myndigheder henvendte sig til Europol, og så landede sagen på skrivebordet hos det danske politi, som efterforskede sagen under kodenavnet "Umbrella". I januar 2018 sigtede politiet 1.004 unge for at have delt eller efterspurgt ulovligt børnepornografisk materiale (straffelovens § 235). De fleste af dem, der blev sigtet, havde delt videoen et par gange, mens enkelte havde gjort det flere hundrede gange. Anklagemyndigheden valgte at rejse tiltale i ni prøvesager. En tiltalt blev frifundet, mens de andre otte blev idømt bøde eller betinget fængsel for enten distribution af børnepornografi eller deling af krænkende materiale. Sagerne ankedes til landsretten, og en sag endte i højesteret, som d. 11. januar 2019 stadfæstede dommen. I både byretten og landsretten blev tiltalte idømt 40 dages betinget fængsel for distribution af børnepornografi. Landsretten afviste at tage stilling til erstatningsspørgsmålet. Det måtte de forurettede bringe videre gennem civile søgsmål. Højesteret har dog bestemt, at tiltalte skal betale 10.000 kroner til den forurettede kvinde og 2.000 kroner til den mandlige forurettede. Det sidste nye i sagskomplekset er, at politiet har rejst 148 nye sigtelser i sagen. I ca. 50 af de nye sigtelser er videoerne blevet delt efter politiets offentlige advarsler om, at det er strafbart, og på trods af den store medieomtale, som sagen medførte i begyndelsen af 2018.

Umbrella-sagen er den mest kendte sag i forbindelse med ulovlig deling af sexmateriale, men langt fra den eneste. Politiken har søgt aktindsigt i antallet af anmeldte § 264 d-sager (deling af krænkende billeder/videoer). Antallet af anmeldelser steg fra 44 i 2011 til 70 i 2013 og 107 i 2015. Antallet mere end fordobledes i 2016 (251 anmeldelser), og det første halve år af 2017 peger i den samme retning (129 anmeldelser). DR har også søgt aktindsigt i § 264 d-sager, og her viser Rigspolitiets gennemgang af § 264 d-anmeldelser fra første halvår af 2016, at omkring 62 % af anmeldelserne handlede om deling af seksuelt krænkende billedmateriale.

En anden kategori af sager, som også hører under overskriften ulovlig billeddeling, er manipulering af billeder. Fænomenet *Deep Fake Porn* er mest kendt som en metode til at indsætte Hollywood-skuespilleres ansigter i pornofilm uden deres vidende og mod deres vilje. Teknologien gør det lettere at (mis)bruge disse muligheder. FakeApp er et eksempel på, hvordan

³² For en meget uddybende beskrivelse af hele sagsforløbet henvises til en artikel af Zetland: <https://www.zetland.dk/historie/sowGG3Wl-aOZj67pz-dbc16>

helt almindelige mennesker i dag kan få adgang til komplekse digitale manøvrer, ifølge professor i kunstig intelligens Anders Kofod-Petersen.³³

Billedmanipulation sker ikke kun med kendisser som ofre; også 'almindelige' mennesker kan blive udsat for denne type chikane. I skrivende stund kører der en retssag i Jylland, hvor en mand er tiltalt for at indsætte ansigter af op mod 18 kvinder i pornografisk materiale. Ansigt-billederne er typisk taget fra kvindernes profiler på sociale medier.

En 23-årig mand fra Midtjylland er tiltalt for at have taget billeder fra unge kvinders sociale medier og manipuleret dem til pornografisk materiale. Billederne er blevet delt på såkaldte fake porn-sites, der er sider med pornografiske videoer og billeder, hvor pornomodellernes ansigter er blevet byttet ud med de unge kvinders. Sagen involverer krænkelser af op mod 18 kvinder. Kvinderne er mindreårige på nogle af de billeder, manden har brugt, og derfor er han både sigtet for at krænke kvinderne ved at have manipuleret deres billeder og for at have medvirket til at dele og distribuere børnepornografi. Mange af billederne er taget fra kvindernes Instagram- og Facebook-profiler.

4.4 Offerprofil

Lidt overraskende er ca. halvdelen af respondenterne i offerundersøgelsen Internetkriminalitet 2017 (Kruize, 2018), der tilkendegiver, at de har været udsat for krænkende identitetsmisbrug, mænd. Fem af de 27 ramte respondenter (19 %) siger, at de kendte personen, der stod bag chikanen (henholdsvis en partner, en ekspartner og tre "anden bekendt"). Offerrisikoen aftager med alderen. De 16-29-åriges offerrisiko er på 1,0 %, mens den falder til 0,4 % for de 30-49-årige og til 0,3 % for de 50-74-årige.

I en rapport om stalking (Justitsministeriets Forskningskontor, 2018) udtalte to ud af tre respondenter, at de kendte stalkeren. Det kunne dreje sig om en (eks)kæreste, arbejdskollega, studiekammerat eller en eller anden, man havde mødt ved en fest. Hos Dansk Stalking Center henvises til Franks (2015), som påpeger, at 90 % af de hævnpornoudsatte er kvinder.

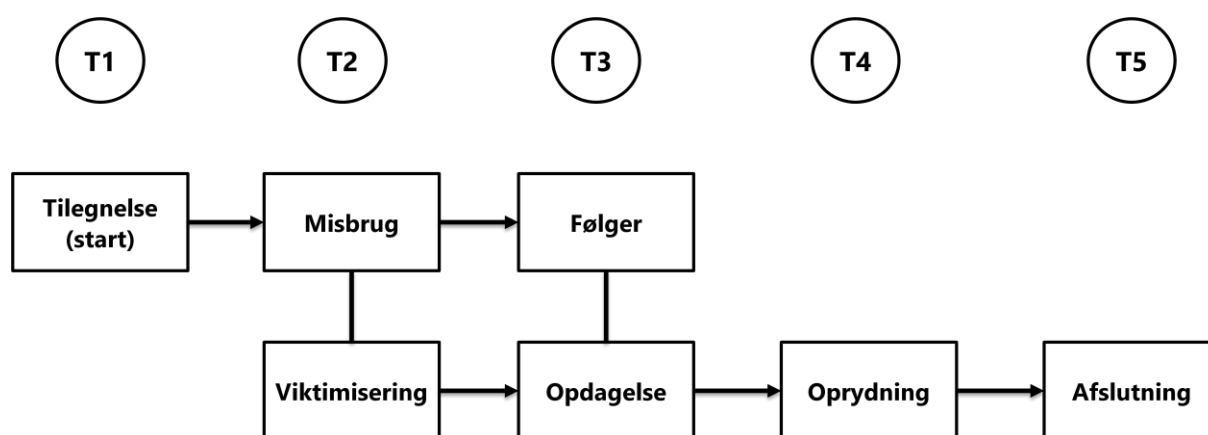
Danske offerundersøgelser er typisk baseret på et repræsentativt udsnit af befolkningen i alderen 15-79 år. Ærekrænkende identitetsmisbrug kan aldersmæssigt ramme bredt, men der er flere tegn på, at netop unge er den største risikogruppe.

³³ I samme artikel påpeger lektor i informationsvidenskab på Københavns Universitet Lars Konzack, at der er rig mulighed for at bruge FakeApp-programmet til både personangreb eller som et politisk våben, der kan sprede propaganda. Men på trods af det er det svært at forbyde programmet. <https://www.dr.dk/nyheder/viden/teknologi/kendis-porno-og-propaganda-kunstig-intelligens-udvisker-graensen-mellem>.

5 Udsattes perspektiv

Langtfra alle identitetsmisbrugsudsatte er klar over, at andre har fået fat i deres oplysninger. Når man har tabt sin pung med et kørekort, er de fleste borgere sig bevidst om, at de har tabt oplysninger, som i teorien kan misbruges. Jo mere de skrider til handling – f.eks. ved at melde det til politiet og kommunen eller aktivere en kreditadvarsel på deres personnummer (se kapitel 7) – jo mindre er risikoen for, at der reelt sker et misbrug, og at de hæfter for tabet, hvis der alligevel er tale om misbrug. Der er dog også mange identitetsmisbrugsudsatte, der slet ikke er klar over, at de har mistet oplysninger. De kan være udsat for phishing eller hacking. Det kan også være, at en af deres nærmeste har misbrugt deres oplysninger, eller at oplysninger er kommet til gerningsmandens kendskab på grund af et databrud³⁴ hos en virksomhed eller en myndighed. Det kan også være, at det drejer sig om oplysninger, som offeret selv har lagt på nettet. Figur 5.1 viser de forskellige faser ved identitetsmisbrug.

Figur 5.1 Faser af identitetsmisbrug i tidsperspektiv



Offeret er sig først viktimiseringen bevidst i det øjeblik, konsekvenserne af misbruget viser sig. Opdagelsen sker, når der trækkes penge fra kontoen, eller når en instans kræver betaling

³⁴ En opgørelse fra Datatilsynet viser, at Datatilsynet, fra den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse, til udgangen af 2018, har modtaget 2.780 anmeldelser af brud på persondatasikkerheden. Af de 2.780 anmeldelser vedrører ca. 80 % mindre end fem berørte registrerede. Datatilsynets opgørelse viser, at 53 % af anmeldelserne af brud på persondatasikkerheden stammer fra private dataansvarlige, mens 44 % af anmeldelserne er fra det offentlige. Over halvdelen af anmeldelserne fra offentlige dataansvarlige stammer fra sikkerhedsbrud i kommuner.

<https://www.kromannreumert.com/Nyheder/2019/02/Disse-brud-paa-persondatasikkerheden-blev-anmeldt-i-2018>

for en vare eller ydelse. Det kan også være, at misbruget opdages ved, at man modtager varer, som man ikke selv har bestilt. I sådan et tilfælde er det ikke lykkedes gerningsmanden at få afleveret varen et sted, hvor han/hun kan modtage den.³⁵ Der kan godt gå et stykke tid, før offeret opdager misbruget. Det kan skyldes, at offeret ikke så ofte ser på kontobevægelser i mobil- eller netbanken, eller at opkrævningen for en ydelse eller et abonnement tager sin tid. Når det handler om ærekrænkende misbrug, er det typisk andre, der gør offeret opmærksom på, at hans/hendes billeder og/eller navn bliver brugt til en profil på et socialt medie, eller at de får uønskede beskeder/henvendelser fra ukendte personer. Denne opdagelsesproces beskrives i afsnit 5.1.

Når offeret har opdaget misbruget, bør oprydningsarbejdet starte. Hvis offeret bliver handlingslammet, ignorerer misbruget eller venter (alt for) længe, bliver det sværere at undgå et økonomisk tab i sidste ende. Oprydningsarbejdet bliver beskrevet i afsnit 5.2.

Efter oprydningen eller manglen på samme kan konsekvenserne af misbruget blive opgjort; økonomiske konsekvenser, psykologiske konsekvenser og hvordan oplevelsen påvirker offerets syn på det danske (rets)samfund. Disse konsekvenser beskrives i afsnit 5.3.

5.1 Opdagelse af identitetsmisbrug

En del af de interviewede ofre for økonomisk misbrug har først opdaget, at der er noget galt, når de har modtaget varer, som de ikke selv har bestilt. At de modtager pakken er et tegn på, at det ikke er lykkedes gerningsmanden at få fat i netop den pakke, men typisk er der bestilt flere varer, og gerningsmanden har fået fat i en del af pakkerne.

Ikke-bestilte pakker

Der dumpede en masse varer ind ad min dør juleaften. Jeg tænker sådan, hvor søren kommer de ting fra. Måske de var en gave fra noget familie. Men så kom der nogle girokort, hvor jeg skulle betale afdrag på de forskellige ting, jeg havde modtaget. Det fortsatte med flere fakturaer og girokort. Jeg finder også ud af, at der er ting, som er afhentet på forskellige døgnbokse i mit navn.

Ikke-bestilte pakker

Det startede med, at det ringede på min dør en dag, hvor jeg tilfældigvis var hjemme. Det var postbuddet med tre pakker til mig. Det kunne jeg ikke helt forstå, eftersom jeg ikke havde bestilt noget. Det var fra Telenor, Bibob og et tredje teleselskab. Det syntes jeg var vildt mærkeligt. Postbuddet sagde, at jeg bare kan afvise at modtage pakkerne. Det takkede jeg pænt ja tak til.

³⁵ I en sag fra 2013 modtog en ung kvinde med posten flere nye iPhones, som hun ikke selv havde bestilt, men som var købt i hendes navn ved hjælp af hendes cpr-nummer. I sådan et tilfælde er der intet tab, for varerne kan bare sendes retur til butikken.

To dage efter fik jeg tre sim-kort med posten. Tillykke med dit nye abonnement og din nye telefon, stod der i brevet. Jeg tænker bare "hvad sker der her". Så jeg ringede ind til de forskellige teleselskaber. Jeg ringer rundt og finder ud af, at det er bestilt igennem mit cpr-nummer med et Mastercard, som ikke tilhører mig, men en mand.

Den næst-hyppigste måde, hvorpå ofre for økonomisk misbrug finder ud af, at en anden bruger deres oplysninger, er gennem ukendte regninger, der bliver sendt til dem.

Ukendte regninger

Der er jo sket det, at jeg opdagede, at der kom nogle sjove regninger ind ad min dør. Der var bl.a. købt et jakkesæt og nogle hudprodukter. Det var igennem en svensk bank, hvor man kunne købe på afbetaling, og det har gerningsmanden gjort. Det er bare mig, som skulle stå for regningen. Sådan var der løbende nogle episoder, hvor jeg fik et brev om, at jeg havde købt forskellige ting. På det telefonabonnement, hvor jeg i forvejen betalte af på min daværende telefon, var der lige pludselig en iPhone på, som jeg aldrig havde købt eller hørt om.

Ukendte regninger

Jeg opdagede det, da der dumpede et brev ind fra TDC med et simkort, jeg angiveligt skulle have købt. Dagen efter kom der et brev fra IDEmøbler, hvor det fremgik, at jeg havde købt møbler for 35.000 kroner. Da brevet fra TDC kom, var jeg på vej ud ad døren, og jeg besluttede mig for at ringe dagen efter til TDC og forklare, at der må være tale om en misforståelse. Dagen efter ligger der et nyt brev i postkassen fra IDEmøbler. Der er et følgebrev med, hvori jeg kan læse, at jeg bl.a. har købt nyt spisebord med seks stole, sofabord og et havebord. Der er også en kopi af en låneaftale gennem Nordea Finans på 35.555 kroner. Så er jeg godt klar over, at der er noget galt. Jeg tjekker min netbank og betalingservice. Der opdager jeg tre betalingsaftaler med Telenor og et finansieringsselskab.

Når det handler om ærekrænkende misbrug, så opdager ofrene for det meste, at deres oplysninger er blevet brugt, efter at de er blevet kontaktet af en bekendt, der gør dem opmærksomme på det. Der kan dermed gå et stykke tid, før misbruget bliver opdaget.

Falsk Tinder-profil

Det er en af mine studerende, som sender mig en kort e-mail. Jeg kan godt mærke på e-mailen, at hun var i tvivl om, om hun skulle skrive den til mig. Det delikate ved situationen er, at hun afslører, at hun har været lidt interesseret i mig. Det er en underlig selvudlevering, der ligger i det fra hendes side, men hun har taget mod til sig og skrevet denne e-mail. Jeg var ekstremt taknemmelig for, at hun skrev til mig.

Jeg har ikke rigtigt kunnet finde ud af, hvor lang tid profilen har været aktiv. Tinder har ikke villet informere mig om det. Der er de her privatlivspolitikker. Tinder må ikke udlevere sådanne informationer. Jeg har hørt, at den har været på spil siden foråret 2015, men jeg har ikke kunnet få det endegyldigt bekræftet. Jeg ved fra de studerende, at de i hvert fald har kendt til profilen i ca. 4 måneder. Jeg fik kendskab til den falske Tinder-profil i december 2015. Jeg ved ikke, om der er andre profiler, som bruger min identitet.

Billede af afdød bror

Min lillebror døde i 2002, og efter et halvt års tid oprettede jeg en mindeside for ham på hjemmesiden mindesiden.dk. I denne forbindelse brugte jeg nogle billeder til mindesiden. Halvandet år efter skriver en pige til mig, at hun synes, hun havde set et billede af min lillebror. Jeg spurgte ind til, hvor hun havde fundet billedet henne. De var fundet på dating.dk.

Misbruget af min lillebrors billeder har været en tilbagevendende begivenhed igennem de sidste 12 år. Det er nøjagtigt det samme billede, som bliver brugt igen og igen. Jeg har et meget stort netværk inde på Facebook, der er mange kvinder og mænd, som er singler på kryds og tværs, som ofte render ind i billedet af min lillebror. Det er ikke kun inde på dating.dk, men på mange forskellige dating-sites.

5.2 Oprydningsarbejde

Når en person opdager, at hans eller hendes identitetsoplysninger er blevet misbrugt, starter den næste fase af processen: oprydningsarbejdet. Det er lidt forskelligt fra sag til sag, hvad der skal gøres, men i de fleste sager om økonomisk misbrug er der i hvert fald tre elementer i oprydningsarbejdet: politianmeldelse, indsigelse over for kreditorerne og spærring af kort eller lignende. Ved ærekrænkende misbrug kan en politianmeldelse komme på tale, men oprydningsarbejdet består i at få fjernet de uønskede beskeder, billeder og/eller profiler fra nettet.

5.2.1 Politianmeldelse

Langtfra alle de respondenter i offerundersøgelsen Internetkriminalitet 2017 (Kruize, 2018), der tilkendegav, at de havde været udsat for identitetsmisbrug, havde anmeldt sagen til politiet. Ifølge Tabel 5.1 har ca. en fjerdedel af ofrene for økonomisk misbrug meldt eller forsøgt at melde sagen til politiet. Det skal bemærkes, at denne undersøgelse også inddrager dem, der ikke har haft et tab på grund af misbruget eller et forsøg på samme. Ved ærekrænkende misbrug har ca. 15 % af ofrene politianmeldt eller forsøgt at politianmelde episoden. Tabellen viser, at politiet afviser en del anmeldelser. Vi vender tilbage til det i afsnit 6.1.

Tabel 5.1 Anmeldelsesadfærd ved identitetsmisbrug

	Økonomisk misbrug	Kortmisbrug	Krænkende misbrug
Ikke anmeldt	76 %	52 %	85 %
Forsøgt anmeldt	5 %	3 %	8 %
Anmeldt	18 %	12 %	7 %
Anmeldt af andre	-	33 %	-

Kilde: Undersøgelsen Internetkriminalitet 2017 (Kruize, 2018)

Nogle interviewrespondenter, der har været udsat for ærekrænkende misbrug, fortæller, at de har valgt ikke at politianmelde sagen, eftersom de synes, at det ikke er en sag for politiet. Det kan være, at de mener, at politiet bedre kan bruge sine kræfter på noget andet.

Billede af afdød bror

Jeg har ikke politianmeldt sagen. Jeg ved ikke, hvad politiet kan gøre i sådan en sag. De skal bruge deres ressourcer på nogle andre ting. Selvom det er en handling, som gør en stødt og ked af det, gør misbrugerens jo ikke nogen skade på den måde.

Eller at den udsatte mener, at sagen ikke er særligt alvorlig.

Falske profiler

Jeg har valgt ikke at gå til politiet, det var ikke vigtigt nok. Og det var sikkert bare nogle tøser, som kedede sig derhjemme, der gjorde det. Sagen er ikke relevant for politiet, og politiet har ikke ressourcer nok til at behandle sådan en sag.

Ved økonomisk misbrug er det mere afgørende at anmelde sagen til politiet, specielt hvis kreditoren kræver en politianmeldelse. Det er (var) ikke altid nemt at anmelde sådan en sag. Nu må det siges, at interviewrespondenten, der citeres nedenunder, var udsat for identitetsmisbrug i 2013, og at politiet de sidste par år har skærpet sin forretningsgang på netop dette område (se også afsnit 6.1).

Økonomisk misbrug

De andre pakker havde jeg afvist med posten, men denne pakke fra 3-mobil var hentet af en anden person. Derefter fik jeg mange problemer med 3-mobil. Jeg ringede ned til en 3-butik, hvor abonnementet var købt, men fik tilsendt flere girokort, som jeg ikke betalte. Herefter ringede jeg til politiet, hvor jeg fik fat i en ikke særligt serviceminded ældre politibetjent. Han fortæller mig, at det ikke er mig, som er den forurettede, men at det er teleselskabet, der var forurettet. Det er derfor teleselskabet, som skal ringe ind og anmelde sagen. Jeg fortæller ham, at det er købt igennem mit cpr-nr., men det kunne han ikke tage sig af. Jeg lagde på og skreg højt i min lejlighed. Herefter ringede jeg op igen og fik fat i en noget mere medfølelsesfuld kvindelig betjent. Hun oprettede heldigvis en sag på mig. Jeg skulle nemlig bruge et sagsnummer for at kunne dokumentere det for selskaberne.

Når offeret kender gerningsmanden, kan det være svært at politianmelde sagen, hvis personen er eller har været en god ven eller kæreste. I nedenstående uddrag fra interviewreferatet beskrives det, at offeret endelig beslutter sig til at anmelde ekskæresten. Politiet optager anmeldelsen, men ellers sker der – til stor frustration for offeret – ikke noget, selvom det er kendt, hvem gerningsmanden er.

Anmelder ekskæreste

Jeg bliver mega-chokeret og ked af det, fordi det er en person, som jeg holder af og har stolet på, trods alt det der er sket. Følelsen af, at han har taget mine personlige oplysninger, lånt pen-

ge i mit navn og sat mig i denne her situation. Tanken om, hvad han ellers har brugt mine personlige oplysninger til, skræmmer mig, idet han er villig til at gøre det her. For mig var der ingen anden mulighed, end at jeg måtte politianmelde ham. Også fordi at jeg havde L'EASY, som stod og truede mig med, at jeg skulle betale de her penge. Selvom jeg ikke nødvendigvis havde lyst til at bringe min ekskæreste i store økonomiske problemer, var jeg nødt til tydeligt at vise, at jeg ikke var indblandet i det her rod. Derfor meldte jeg ham til politiet.

Så udover at jeg var virkelig ked af det og følte mig svigtet, følte jeg mig også rigtig bange, idet han var psykisk ustabil. Jeg var meget bange for, at han ville få at vide, at jeg havde meldt ham til politiet. Hvad kunne han finde på at gøre mig? Jeg var rimeligt bange.

Min sag startede i en bunke på et skrivebord i Station City. Jeg ringede ind til dem igen efter et halvt år. Men politiet fortæller, at de er ved at omstrukturere afdelinger og derfor har travlt. Vi behandler din sag så hurtigt som muligt. Derefter fulgte jeg op på sagen hvert halve år, men politiet blev ved med at komme med den samme undskyldning. Jeg klagede til politiet, statsadvokaten og til sidst til ombudsmanden, men jeg har ikke fået medhold i nogen af mine klager.

5.2.2 Indsigelse

Når regninger falder på dørmåttten, eller når der bliver trukket et beløb fra ens konto på grund af identitetsmisbrug, skal der gøres indsigelse mod regningen eller træk på kontoen. Det er vigtigt, at der gøres indsigelse ret hurtigt, for ellers er der en reel chance for, at en forsinket reaktion bliver betragtet som et tegn på, at personen selv ikke er helt uskyldig. At gøre indsigelse kan være en belastning for en del af de udsatte. En af respondenterne siger det således:

Jeg skulle selv lave det meste af arbejdet. Hvis man ikke er ressourcestærk, er man på bar bund. Man skal reagere, skrive breve osv. Ellers mistænkeliggør man sig selv. Det er svært, hvis man f.eks. ikke taler flydende dansk, ikke er fastholdende osv.

En politirespondent fortæller om to borgere, der havde været udsat for identitetsmisbrug, og som ikke rigtig havde overskud til at gøre indsigelse, men han understregede for dem, at det var vigtigt at gøre det.

Jeg har haft to tilfælde, som har været udsat for identitetsmisbrug. De blev nærmest socialt handicappede, fordi de ikke turde gå uden for en dør. De blev så påvirkede over at få alle de regninger fra firmaer, der ikke troede på dem. Hele den der mistro drev dem til vanvid. Jeg brugte meget energi på at vejlede dem om, hvordan de skulle gøre. Mit råd var, at de altid skal reagere på noget, som ikke vedrører dem.

Hvis man ikke reagerer på regninger, eller kreditoren ikke tror på, at ens identitet er blevet misbrugt uden ens vidende og samtykke, kan sagen blive sendt til en inkassovirksomhed. Ifølge loven skal kreditoren mindst én gang advare om, at sagen bliver sendt til inkasso. I det øjeblik, der bliver sendt rykkere (med gebyr), og sagen bliver sendt til inkasso, kommer der

flere udgifter på regningen. Der kommer et inkassogebyr på, som er lovreguleret, og hvis sagen ender i civilretten og/eller fogedretten, kommer der yderligere gebyr på regningen. Vi vender tilbage til de sager, der ender hos en inkassovirksomhed og muligvis i retten, i afsnit 6.3.

Interviewrespondenterne har forskellige erfaringer med at gøre indsigelse. Flere respondenter melder, at kreditorerne medvirker uden problemer, som i nedenstående eksempel.

Jeg ringede til de forskellige firmaer. De kunne blot afskrive mig fra regningen, hvis jeg politianmeldte det og gav dem journalnummeret. Det gjorde jeg så. Derefter har jeg ikke hørt mere tilbage fra dem. Alle firmaer har været ret forstående. Garanteret også fordi det har været så meget oppe i medierne den sidste tid. Så de ved selvfølgelig godt, at det kan ske.

I andre tilfælde kræver det mere energi af offeret, før kreditoren er villig til at droppe sit krav. Imens kommer der flere rykkere ind ad brevsprækken.

Jeg ringede så til 3-mobil og sagde, at jeg nu havde anmeldt sagen hos politiet. Abonnementet ville jeg gerne have lukket, eftersom jeg ikke kender noget til det. Det kunne de desværre ikke gøre. De skulle bruge en masse papirer. Jeg blev ved med at modtage regninger fra 3-mobil og rykkere. Og jeg fortsætter med at ringe og klage. På meget mystisk vis blev telefonkøen længere og længere, for hver gang jeg ringede til dem. Til sidst fik jeg papirer, hvor de truede med at politianmelde mig. Jeg var faktisk ligeglad, jeg ville bare have det ud af verden. Jeg tænkte, at det var bedre at blive politianmeldt end at havne i RKI.

Det her stod på i over et halvt år, men til sidst lukkede de mit telefonnummer, fordi jeg ikke havde betalt regningerne. Beløbet var løbet op i omkring 10.000 kr. Jeg snakkede med en fra 3-mobil, som sagde, at de ville sende mig et brev med frankeret svarkuvert. Her skal du udfylde en tro- og love-erklæring. Jeg udfyldte det og sendte det tilbage til 3-mobil. Så gik der en ca. 14 dage, så fik jeg en ny rykker. Jeg ringede derfor til 3-mobil og fortalte, at jeg har sendt denne her svarkuvert ind til dem. Han fortæller så, at der står forkert adresse på kuverten. Ham, jeg havde i røret, hjalp mig så med at afslutte sagen.

5.2.3 Spærring

Når ens betalingskort eller NemID-nøglekort er blevet misbrugt, er det vigtigt, at dette kort bliver spærret med det samme. Det er også enkelt at gøre. Det kan også være, at et betalingskort bliver spærret præventivt. Nets har et overvågningssystem til at identificere misbrug og misbrugsmønstre vedrørende betalingskort. Eksperter følger og overvåger døgnet rundt samtlige korttransaktioner. Systemet er sat op til at fange usædvanlige hændelser; f.eks. et kort, der bliver brugt mange gange efter hinanden, hvilket tyder på, at kortet er stjålet. Systemet advarer også, hvis det samme kort – inden for samme tidsrum – bliver brugt både på Storebæltsbroen og i Thailand. Det betyder, at kortet er kopieret og bliver lukket med det

samme (Kruize, 2009). Og så kan mange kort blive udskiftet præventivt på én gang på grund af muligt misbrug. I september 2018 meddelte Nets følgende:

14.000 danske forbrugere vil de kommende dage blive kontaktet af deres bank med besked om, at de skal skynde sig at annullere og smide deres gamle hævekort ud, og at de vil få tilsendt et nyt. Der er nemlig en begrundet mistanke om, at data på de 14.000 kort er i hænderne på kriminelle hackere. Det oplyser Nets, der håndterer transaktionerne og varetager misbrugsovervågning. "Vi kan se, at der er nogle kriminelle, der over en periode på en specifik hjemmeside har stjålet kortoplysninger på en relativt stor mængde kort", siger Kaspar Kock Kristensen, ansvarlig for misbrugsbekæmpelse i Nets.

Der er dog også identitetsdokumenter, der ikke kan spærres. Det er indtil videre ikke muligt at spærre et kørekort eller et pas. Disse dokumenter kan meldes stjålet, men de kan stadig anvendes af andre i mange situationer. En af interviewrespondenterne ønsker, at der var flere muligheder for at spærre stjålne kort eller identitetsbeviser. Hun siger: "Det offentlige burde lade sig inspirere af bankernes håndtering af stjålne betalingskort. Der ligger et hav af sygesikringskort fra hver gang, folk er flyttet, har tabt deres pung eller mistet deres pas i udlandet. Det bør man kunne spærre".

5.2.4 Sletning af billeder, profiler og mere fra nettet

Hvordan billeder mm. slettes fra nettet, kommer vi ind på i næste kapitel, men her beretter vi om udsattes erfaringer med sletning af uønskede billeder og lukning af falske profiler. Når det handler om de kendte platforme, som Facebook, Instagram og Tinder, så er erfaringerne for det meste positive. Det vil sige, at det lykkes at lukke den falske profil. Det kræver en form for dokumentation at bevise, at profilen er falsk. Afhængigt af platformen kan det også være nødvendigt at skrive en anmodning på engelsk – hvilket kan være en forhindring for nogle. En af interviewrespondenterne har lukket en falsk Tinder-profil. Han beskriver processen, som følger:

Jeg kom i kontakt med Tinder ved at skrive til dem med det samme, jeg fandt ud af, at det her stod på. Jeg oprettede en sag inde på deres websupport-hjemmeside. Jeg skulle ikke selv først oprette en profil, men man skulle angive information, som om man havde en profil. Man skulle opgive, hvilken version af Tinder man bruger, men det kunne man godt gøre uden at skulle logge ind. Da jeg så havde været i kontakt med Tinder og havde skrevet en 5-6 e-mails med dem, hvor de skulle have screenshot, beskrivelser, og jeg skulle bevise over for dem, at jeg var mig; alle sådan nogle sikkerhedsprocedurer. Det her foregik på engelsk. Dialogen stopper med, at Tinder får lukket ned for profilen, sådan forholdsvis hurtigt, omkring 10 dage.

Det er dog mere besværligt eller umuligt at fjerne indhold på bestemte datingsites og udenlandske (pornografiske) sider. En af respondenterne forsøger at slette en profil med hendes

billede på den daværende datingsite matchclub.dk. De svarede dog aldrig på hendes henvendelser. En journalist fra Jyllands-Posten har haft kontakt med en medarbejder hos matchclub.dk, der fortæller, at han og andre medarbejdere blev opfordret til at kopiere billeder, som kunne bruges i fiktive profiler på datingsiderne.

5.3 Konsekvenserne af identitetsmisbrug

I dette afsnit ser vi på både økonomiske og psykiske konsekvenser af identitetsmisbrug. Og så ser vi nærmere på, hvordan oplevelsen har konsekvenser for udsattes syn på det danske retssamfund.

5.3.1 Økonomiske konsekvenser

For alle identitetsmisbrugsudsatte gælder det, at de skal bruge tid til at reagere på misbruget. Det kan være i form af at ringe/skrive til kreditorerne, kontakte politiet, kommunen og/eller banken eller søge kontakt til sociale medier. Så selvom misbruget muligvis ikke har direkte økonomiske konsekvenser, har det indirekte økonomiske omkostninger. Der er respondenter, der fortæller, at de har brugt så meget tid (energi), at de ikke var i stand til at arbejde i nogle dage/uger.

Jeg har ikke arbejdet i tre uger. Har brugt al min tid på at ringe rundt; til finansieringsselskaber, til politiet. Jeg var nede ved politiet flere gange og har været ved kommunen flere gange.

Det kan også være, at offeret (delvist) hæfter for det økonomiske tab, der er opstået. Det gælder typisk, når NemID-oplysninger er misbrugt. Hertil vender vi tilbage i næste kapitel. Endvidere kan det være, at offeret har købt sig til f.eks. advokatbistand. Vi er dog ikke stødt på eksempler på, at offeret har betalt for (advokat)bistand.

5.3.2 Psykiske konsekvenser ved økonomisk misbrug

Udover økonomiske konsekvenser kan identitetsmisbrug få psykiske konsekvenser. Når det handler om økonomisk misbrug, handler det om bekymringer for at miste (mange) penge og bekymringer over, hvordan misbruget kan stoppes. Det kan resultere i stress, søvnløshed og i sidste ende en sygdomsmeddelelse til ens arbejde. En respondent beskriver sin første reaktion således:

Når jeg fatter, at der blev svindlet i mit navn og for hvilke beløb, stivner jeg, og det løber mig koldt ned ad ryggen. Det er mange penge, og der står jo mit navn og adresse på papiret. Jeg aner simpelthen ikke, hvad jeg skal gøre, og er vildt bange for, at jeg kommer til at betale for alt det, der er blevet købt. Jeg lå søvnløs om natten og var livsens ræd for, at de også skulle gå i

banken for at tømme min konto der. Gulvtæppet blev hevet væk under en. Når rudekuverter kommer, ser man det hele smuldre for sig. Jeg havde sparet op til et hus. Det hele gik op for mig. Skulle jeg starte fra scratch igen? Det var ligesom at få en knytnæve i maven.

Et par dage senere kom hun over det første chok. Eller som hun beskriver det: "I tre dage var jeg offer. Så rejste jeg mig igen". Men oplevelsen sidder i hende og har sat spor for lang tid/livet. Hun beskriver det selv således:

En grusom oplevelse. Der er stadig fare for misbrug, for mit kort er stadig derude. Hver gang, jeg åbner postkassen, holder jeg vejret og håber, at der ikke kommer en ny rudekuvert. Tanken om, at jeg skulle miste min pung igen får mig til at kaste op. Kan ikke klare tanken om, at jeg skulle gennem noget lignende igen. Jeg har det forfærdeligt med, at selv om kvinden bliver fanget, så florerer mine data stadig rundt. Jeg skal altid være påpasselig. Der er ikke noget, der kan stoppe det, da man jo ikke kan spærre sit sygesikringskort. Jeg frygter, at der sker noget om 3 år. Bange for, at jeg har glemt noget. De kan f.eks. også leje en bil. De har stadig mit kørekort og sygesikringsbevis.

De fleste respondenter har dog en lidt mere afdæmpet reaktion på det økonomiske misbrug, men i starten er de fleste bange for, at der kommer flere rudekuverter.

Jeg blev i starten lidt paranoid af hele situationen. Hvis jeg skulle udfylde en blanket med cpr-nr., var jeg lidt bange for, at andre ville se mit cpr-nr., hvis den blev væk. Jeg brugte så mange kræfter på det. Jeg fik tilmed skiftet adresse til mine forældre, så posten kom dertil. Her vidste jeg, at der ville være nogen hjemme. Jeg fik nærmest "postkasse-skræk". Jeg turde ikke åbne min postkasse i flere måneder, for tænk, hvis der lå flere rykkere eller lignende. Jeg var mest paranoid i starten, men eftersom det kun varede omkring en uge, hvor jeg fik post, som jeg ikke kendte til, forsvandt tanken løbende.

5.3.3 Psykiske konsekvenser ved ærekrænkende misbrug

Når der er tale om ærekrænkende misbrug, kan der også være psykiske konsekvenser, der fører til stress, søvnløshed og angst, men det bunder i bekymringer for reaktioner og fordommelser fra nærmeste, venner eller andre omgivelser. Et offer, hvis oplysninger blev delt med opdigtede sexydelser, har søgt psykologhjælp.

I dag sover C. stadig dårligt om natten, og hun er angst for at besvare opkald fra hemmelige numre, fordi alle mændene med undtagelse af én ringede fra hemmeligt nummer. Adskillige sorte ringbind vidner i dag om det retslige og psykologiske efterspil, som sagen siden hen har haft for hende. Identitetstyveriet har også fået et fysisk efterspil for C., der pga. de aldrig stillestående tanker har daglige hovedpiner, som forårsager myoser. Foruden ugentlige psykolog-samtaler har hun derfor også ugentlige aftaler hos en fysioterapeut.

En respondent, som blev udhængt som pædofil, efter at hans billeder var blevet misbrugt på et socialt medie, har søgt medieopmærksomhed til at fortælle sin historie. Misbruget førte i sidste ende til en sygemelding i et halvt år.

Og så havde politiet lige pludselig nok ressourcer nok til at gå ind i sagen. Det er utroligt, at man skal i medierne, før politiet tager affære. Først var jeg i P3-nyhederne i radioen og fortælle om situationen, og derefter ringede telefonen stort set konstant. Jeg var i mange medier, Aften-showet, TV2 osv. Da jeg var på vej ned til toget efter et interview, var der en, som råbte 'klamme svin' til mig. Jeg blev kaldt alle mulige ting, 'billige stodder'. Jeg begyndte at isolere mig mere og mere. Jeg var bange for at gå udenfor. Jeg tænkte på, om der var nogen, som ville slå mig ned. Jeg var rigtigt bange. Da jeg endelig går udenfor, var der en mor, som kom gående med sit barn mod mig, og så kunne man bare se panikken i hendes øjne. Og de skyndte sig over på den modsatte side af vejen og over på det modsatte fortov. Efter denne episode begyndte jeg at isolere mig mere. Et par uger efter begyndte det små småt at ebbe ud med beskeder. Det hele endte med, at jeg fik stress og blev sygemeldt i et halvt år. Nu er jeg videre, men det sidder altid i mig. Jeg får en klump i maven, hver gang jeg ser andre blive udsat for lignende.

Nu er begge ovenstående eksempler ret alvorlige sager, men også – sandsynligvis – mindre alvorlige misbrugssager kan have psykiske konsekvenser, således som nedenstående to eksempler vidner om.

Falsk Tinder-profil

Jeg anser mig selv som psykisk ret robust. Jeg havde ikke brug for at være sygemeldt i en uge, efter det her stod på. Jeg blev selvfølgelig rigtigt chokeret og ked af det, da jeg fandt ud af, at det her havde fundet sted, og trak stikket i et par dage for at sunde mig. Det var voldsomt at få at vide.

Flere falske profiler

Meget ubehageligt, for det er ukendt, hvem der står bag den falske profil. Hun får tilsendt på Ask en mappe med hendes billeder, som hun har lagt op igennem årene. Dermed har hun en fornemmelse af, at en person, der står bag den falske profil, følger hende i længere tid. Står til i et år. Først for en måned siden har hun informeret sin mor. Bange for at gå ud ad døren; bange for at blive voldtaget, på grund af hvad der skrives i hendes navn på Ask.

Psykolog Anne Lundgaard påpeger³⁶, at identitetsmisbrugsudsatte kan føle, at de mister kontrollen over deres liv. Den manglende kontrol kan medføre en næsten eksistentiel angst.

Det er meget grænseoverskridende og psykisk problematisk, fordi man som offer spekulerer på, hvad andre tænker om en, og om de ser en på samme måde, som man ser sig selv. Det kan give ofrene så mange bekymringer, at det fører til en konstant uro i kroppen. Uroen bringer kroppen i et alarmberedskab, hvor den opsluges af følelsen af at være klar til at flygte eller kæmpe. Når

³⁶ Se: <http://viden.jp.dk/undervisning/sites/penge/indsigt/artikler/default.asp?cid=153092>

alarmberedskabet fylder alt, mister man det, der giver mening i livet, såsom venner og familie. De gode ting i livet er der stadig, men man overser dem, fordi kroppen er stresset. Det tager lang tid, men ofre for identitetstyveri skal forstå, at sandsynligheden for, at det sker igen, er lille, og at deres alarmberedskab derfor er alt for stort.

5.3.4 Syn på retssystemet

For nogle udsatte har identitetsmisbruget også som konsekvens, at deres tro på Danmark som et retssamfund lider et knæk. Selvom en del af respondenterne giver udtryk for, at de har forståelse for, at politiet ikke har ressourcer til at efterforske deres sag, kan en afvisning – af at optage en anmeldelse – føre til mindre tiltro til myndighederne og det danske samfund som helhed.

Tryghed er vigtig. Hjemmet er helligt. At stole på, at tingene fungerer, og på, at når der er noget galt, så kan jeg henvende mig til myndighederne, som så kan hjælpe mig. Jeg sidder tilbage med en følelse af magtesløshed og af, at jeg er blevet afvist.

Myndighedernes troværdighed lider også et knæk, hvis et offer bliver konfronteret med forskellige synspunkter eller får indtryk af forskelsbehandling. Når man anmelder et identitetsmisbrug til politiet, er der fra politikreds til politikreds forskel på, hvordan de håndterer disse sager (se også afsnit 6.1), men respondenterne oplever også modsatrettede udmeldinger inden for den samme politikreds/station.

Det har været en interessant oplevelse og erfaring for mit eget vedkommende, hvor forskellig information man kan få ved at kontakte en offentlig instans som for eksempel politiet. Hvis jeg tirsdag eftermiddag får fat i Anders Nielsen, får jeg et svar. Ringer jeg torsdagen ugen efter og snakker med Niels Hansen, får jeg et andet. Det med at der er en intern uoverensstemmelse omkring, hvad der er hvad, og hvad man kan stille op i de her sager – det synes jeg var overraskende. Jeg kan selvfølgelig godt forstå, at der er forskellighed. Politiet er en stor organisation, men at det decideret var i øst og vest, det jeg fik at vide, forstår jeg ikke.

Endelig kan udsattes syn på det danske retssystem komme under pres, hvis de har indtryk af, at deres sag bliver syltet, og af, at en klage over sagsbehandlingen ikke bliver hørt eller bliver overhørt.

Det er hele tiden mig, der skal opsøge politiet og hele tiden rykke og spørge ind til, om de har fundet ud af noget. Der er en masse dårlige undskyldninger. Man bliver ligesom spist af med forklaringen "at det kan vi desværre ikke, det er der nogle andre, som skal se på". Man føler sig meget bokset rundt i et system uden ende – et bureaukratisk helvede.

Hver gang, jeg har fået svar tilbage fra en af mine klager, er jeg bare blevet mere og mere harm. Især over at det ingen konsekvenser har fået for min ekskæreste. Jeg synes også, det er underligt, at politiet ikke har gjort mere, idet jeg vidste, præcis hvem gerningsmanden var.

6 Aktørernes syn

I dette kapitel er aktørernes syn centralt. En aktør er en person, der erhvervsmæssigt har kontakt med identitetsmisbrugsudsatte. Det kan være personer, der arbejder hos politiet, anklagemyndigheden eller domstolen, i en inkassovirksomhed eller en virksomhed, der tilbyder forbrugslån, eller advokater. Men det kan også være en person, der arbejder i et forsikrings-selskab eller en instans, der tilbyder hjælp til identitetsmisbrugsudsatte.

Aktørerne har formentlig et bredere syn på identitetsmisbrug end udsatte. De ser flere forskellige tilfælde af misbrug og kan dermed bedre se bestemte tendenser og mønstre. Aktørernes syn er præsenteret efter fire emner:

1. Politianmeldelse
2. Efterforskning
3. Hæftelse for tabet
4. Sletning.

6.1 Politianmeldelse

For nogle år siden skete det regelmæssigt, at politiet ikke ville optage en anmeldelse om økonomisk identitetsmisbrug, med den begrundelse, at personen juridisk set ikke var forurettet. Hvis man ikke hæfter for tabet, er man ikke forurettet i sagen. Det stillede personen, hvis identitet var blevet misbrugt, i en svær situation over for kreditorerne. Kreditorerne spørger typisk som det første, om sagen er politianmeldt. Derfor er det nu internt i politiet besluttet, at de altid optager en anmeldelse. Herunder et eksempel på det brev, som politiet i en af landets politikredse sender til ofre for økonomisk identitetsmisbrug.

Vedr. anmeldelse om misbrug af identitet

Politiet har modtaget din anmeldelse om misbrug af identitet, foreløbig til køb af varer hos X og Y. Din anmeldelse er registreret under ovenstående journalnummer. Misbrug af identitet er ikke selvstændigt kriminaliseret i dansk lovgivning. Handlingen kan derimod være strafbar som bedrageri i forhold til leverandørerne af varerne. Du kan eventuelt henvise de firmaer, som nu og i fremtiden måtte have leveret varer i dit navn til en ukendt person, til, at de skal foretage en anmeldelse – gerne med henvisning til ovenstående journalnummer. Der vil således på det foreliggende ikke blive foretaget yderligere i anledning af din anmeldelse.

En rundringning til landets politikredse viser, at politiet alligevel håndterer disse anmeldelser forskelligt, alt efter hvilken politikreds der er tale om.³⁷ Det gør ikke den store forskel for anmelderen, men registrering under et 'ikke skarpt' Polsas-nummer (dvs. ikke som anmeldelse) giver formentlig mindre incitament til efterforskning end et skarpt nummer. Det har i hvert fald konsekvenser for kriminalstatistikken, som kun viser sager, der er registreret under et skarpt nummer.

En af politirespondenterne forklarer, hvorfor de gerne vil have en anmeldelse fra den forurettede part og ikke borgeren, hvis identitet er misbrugt:

Når vi får en anmeldelse fra en borger, som har fået misbrugt sine oplysninger fra sit kreditkort, så er det ikke borgeren, som er den forurettede, fordi kunden får pengene tilbage fra webshoppen eller banken. Så vi vil helt klart helst have anmeldelsen fra den forurettede, som ikke er borgeren, men banken eller selskabet. Det gør det lettere for os. Den kunde, der har fået misbrugt sine oplysninger, har sjældent de oplysninger, vi som politi har brug for, og kunden/borgeren er som sådan ikke en rigtig part i sagen.

Retningslinjerne er dog, at politiet skal oprette en sag, når de alligevel får en anmeldelse fra en borger i sådan en sag. Det er et krav fra rigsadvokaten, at en anmelder får en slutnings-skrivelse i de her sager. Og det betyder, at borgerens anmeldelse skal have et såkaldt skarpt sagsnummer. Borgeren kan medbringe dette journalnummer til banken eller lignende. Disse retningslinjer bliver dog ikke altid efterlevet i praksis. En af politirespondenterne forklarer det således:

Der er rigtigt mange ansatte i servicecentret, der alle skal kunne mange ting. Det er svært at ensrette det, og det er tilmed et relativt nyt område, hvorfor der sommetider sker fejl. Der er ikke en fast etableret lovgivning på dette område. Når noget ændres, så skal alle have det at vide, før den nye praksis er udbredt.

I en anden politikreds vælger man dog at arbejde med et såkaldt undersøgelsesnummer, når en borger anmelder sagen. Respondenten begrundet det således:

Vi optager en anmeldelse, hvis personoplysninger er misbrugt, men personen ikke selv hæfter for den økonomiske skade. Det er en klassisk opstart på identitetsmisbrug – eller kan være det. Det vil sige, at det, vi gør som politimyndighed til at starte med, er, at vi altid optager en anmeldelse, hvis der er mistanke om et kriminelt forhold. I de her sager opretter vi et undersøgelsesnummer. Det er ikke sikkert, vi altid ved, hvad vi har med at gøre. Det handler også om at give den forurettede/anmelderen en "ro på". Nu har politiet optaget en anmeldelse. Det journalnummer, som vi giver til forurettede, kan de bruge til bankerne eller lånefirmaerne, som de hen-

³⁷ Vi må antage, at de forskellige praksisser (delvist) hører fortiden til efter oprettelse af LCIK i januar 2019 (se også fodnote 5).

vender sig til. Så kan låneinstituttet bruge journalnummeret til at sende en anmeldelse ind til politiet. Det er, så vi sikrer os, at vi ikke dobbeltregistrerer anmeldelser.

En tredje politirespondent tilkendegiver, at politiet ikke har en fasttømret arbejdsgang. Det afhænger af den konkrete sag.

Vi registrerer alle henvendelser. Det er vi forpligtede til. Typisk vil der næsten altid være et andet forhold, som vi vil registrere det på. For eksempel noget tyveri eller indbrud. Og så kunne vi lave en undersøgelsessag. Det er forskelligt, om det bliver registreret som en undersøgelsessag eller på et skarpt nummer. Det kommer an på den konkrete sag og en vurdering hver gang.

Et undersøgelsesnummer er ikke et skarpt journalnummer og figurerer dermed ikke i statistikken. Så hvis butikken eller banken ikke anmelder sagen, optræder sagen ikke i politiets anmeldelsesstatistik.

I en af politikredsene opretter man for hver henvendelse et skarpt journalnummer. Det kan føre til, at en sag kan tælle flere gange i kriminalstatistikken. Respondenten forklarer dette fænomen således:

I nogle tilfælde får vi tre sager på én hændelse. Det kan være, at der i første omgang kommer en ejer af et betalingskort, som er blevet misbrugt. Herefter kan det være, at banken efterfølgende anmelder det samme forhold, fordi de går ind og dækker kundens tab. Hvis banken så har lavet en charge back fra et internetfirma, hvor betalingskortet er blevet misbrugt, laver firmaet også en anmeldelse. Nu har vi tre anmeldelser på tre forskellige journalnumre på den samme hændelse. Vi samler selvfølgelig sagerne, men hvis man begynder at føre noget statistik på disse bedragerisager, så har vi tre tilfælde i stedet for ét tilfælde. Det er lidt svært at gå ind og trække statistik på de her sager.

Ærekrænkende identitetsmisbrug

Beslutningen om, at politiet skal optage anmeldelsen, gælder dog kun økonomisk identitetsmisbrug. Når det kommer til ærekrænkende misbrug, er det langt fra sikkert, at politiet vil optage anmeldelsen. Begrundelsen herfor er ikke – som det gælder for økonomisk misbrug – at offeret ikke er den forurettede part, men at forholdet ikke er strafbart, eller at det ikke er underlagt offentlig påtale (men privat påtale). Når det handler om f.eks. deling af nøgenbilleder af mindreårige, kan sagen anmeldes og efterforskes som børneporno, men når det handler om en falsk oprettet profil på et socialt medie, er der tale om ærekrænkelser, der som udgangspunkt er underlagt privat påtale. En politirespondent forklarer det på følgende vis:

Vi oplever ikke ret ofte, at der kommer sådan en anmeldelse. Men hvis det sker, er der typisk et hævnmotiv på grund af et brudt forhold. Det er typisk mænd, der hævner sig på kvinder. Om vi efterforsker det aktivt afhænger bl.a., om der er overtrådt noget. Det er ikke så meget under straffelovens bestemmelse om ærekrænkelser, de her sager efterforskes, men f.eks. børneporno-

grafi, hvis det handler om nøgenbilleder af en under 18 år. Vi ser ikke så mange anmeldelser. Ikke fordi det ikke sker ofte, men fordi man selv prøver at ordne det ved at kontakte Facebook for at lukke profilen. Vi ser kun toppen af isbjerget.

En anden politirespondent tilføjer: "Hvis ikke der er noget strafbart, optager vi ikke en anmeldelse, men vi registrerer det selvfølgelig".

Billeddelingssager er undergivet betinget offentlig påtale. Det vil sige, at offeret selv skal henvende sig til politiet. En politirespondent påpeger, at denne betingelse kan være til gavn for den person, der figurerer på billedet, og giver følgende eksempler:

Det kan godt være, at jeg tænker, du er krænket over et billede, men det er ikke sikkert, du selv tænker det. Det kan også være, du er en teenagepige på 17 år, der helst ikke vil have, at dine forældre finder ud af, at det her billede eksisterer. Derfor har du ikke det store behov for, at politiet kommer hjem og banker på hos dig, fordi nogle andre har anmeldt dit billede.

6.2 Efterforskning

De fleste politirespondenter gør klart, at sagen ikke bliver efterforsket, hvis der ikke kommer en anmeldelse fra den 'reelle' forurettede, det vil sige dem, der hæfter for tabet i økonomiske misbrugssager. I en af kredsene opleves det, at de får for mange af disse anmeldelser. De tilkendegiver, at de ikke kan følge med i stigningen i antallet af anmeldelser. Derfor prøver de i samarbejde med de såkaldte professionelle anmeldere, det vil sige virksomhederne, at nedbringe antallet af anmeldelser ved at gennemgå og ændre deres procedurer.

Vi vil gerne hjælpe der, hvor det giver mening. Hvis vi får færre sager ind, kan vi gøre en større indsats i de sager, i stedet for en mindre indsats i et bredere antal sager, hvis vi får alt for mange anmeldelser. Vi vil helst arbejde der, hvor det gør gavn. Så hvis vi kan nedbringe antallet af anmeldelser, vil vi gavne mere der, hvor folk har brug for vores hjælp.

Også en anden politirespondent peger på (for) mange sager og prioritering. Hvis forretninger ikke selv vil gøre en indsats, er begejstringen hos politiet heller ikke for stor. Det illustreres på følgende måde:

Jeg har haft fat i nogle af de store butikskæder for et år tilbage, hvor jeg spurgte, hvorfor de blev ved med at anmelde de her sager. Svaret var, at det er et princip, men de vil ikke lægge hindringer i vejen for kunderne. Derfor har de en politik om, at de anmelder det misbrug, der er, men de tjener meget i forvejen, så det betyder ikke noget for deres omsætning. Det er en barsk holdning at have til identitetsmisbrug, og det er irriterende for os. Vi prioriterer ikke sagerne særligt højt, når det er med den indgangsvinkel.

På den anden side er der sager, der netop bliver prioriteret. Den samme respondent siger: "Jeg har lige nu skadesløse borgere på beboere steder, hvis identitet er misbrugt. Det rammer mig hårdt. De sager gør vi noget ved, så snart vi får kendskab til dem".

Det overordnede billede er, at politiet i princippet visiterer alle sager, men først efterforsker en sag, når der er efterforskningsmuligheder og ressourcer til stede. Når der er overført penge – f.eks. ved et lån – så er det forholdsvis enkelt at følge pengesporet. Det ender for det meste ikke hos bagmanden, men giver et spor at arbejde efter.

Hvis en identitet er blevet misbrugt til flere forskellige ting og over længere tid, er der en chance for, at de afslører sig selv. Især hvis der er tale om lån, for så går vi ad pengesporet. Til hvilken konto er pengene udbetalt, det er typisk ikke gerningsmandens konto. Det vil være en konto, som på en eller anden måde har en forbindelse til gerningsmanden.

Opklaring af sager ved at følge pengesporet giver mening, så længe det handler om 'lokale knægte', hvor penge er overført til danske pengeinstitutter. En anden efterforskningsmetode er overvågningsbilleder. Hvis der er købt eller bestilt en vare i en fysisk butik, kan gerningsmanden identificeres den vej rundt. Elektroniske spor i form af IP-adresser betragtes som mindre værdifulde, eftersom mange gerningsmænd benytter sig af dynamiske IP-adresser, en proxyserver³⁸ eller en computer på et offentligt sted som f.eks. et bibliotek.

Sagen skal have en vis tyngde, før politiet indhenter oplysninger via retsanmodning. For nogle år siden var en IP-adresse ret præcis i forhold til, hvilken computer der blev brugt. Nu kan alle finde ud af at bruge en proxyserver, og dermed er det svært at benytte IP-adressen. Det kan ikke stå alene. Det har tabt sin værdi.

Efterforskningen bliver mere kompleks, når sporene viser, at gerningsmanden sidder i udlandet. Det kan hurtigt være grund til at henlægge sagen.

Når efterforskningen viser, at misbruget er sket fra en server nede i Afrika, så ved vi udmærket godt, at chancen for at finde gerningsmanden nede i Marokko er ganske lille. Chancen for at få ham udleveret er meget, meget lille – næsten ikke-eksisterende. Vi slutter ofte sagerne, hvor de elektroniske spor fører til nogle steder, hvor vi ved, at et samarbejde er uopnåeligt.

Ærekrænkende identitetsmisbrug

Identitetsmisbrug med et økonomisk sigte efterforskes af politiets enheder, der beskæftiger sig med økonomisk kriminalitet, mens ærekrænkende misbrug typisk bliver lagt over til en afdeling for almen efterforskning. En politirespondent forklarer begrundelsen for denne opdeling:

³⁸ En proxyserver er et serverprogram, der optræder som en stedfortræder på internettet. En åben proxyserver kan bruges af alle og har til formål at give en anonymiseret adgang til internettet.

Hvis man ser på sagerne omkring økonomisk kriminalitet, så er det ikke vores opfattelse, at personer, som får misbrugt deres oplysninger, at det er for at ramme eller skade den enkelte person. Der bliver deres identitet brugt som redskab for at opnå noget andet.

Den anden del kan det være ekskærester eller folk, som vil en ondt, som misbruger deres identitet eller misbruger billeder af dem på nettet. Det er en anden kategori, hvor vi bevæger os over i nogle andre paragraffer i straffeloven.

Der kan sættes spørgsmålstegn ved denne påstand; om opdelingen i praksis er så skarp. Efter vores mening er det ikke altid klart, om f.eks. misbrug af billeder har chikane til formål. Man kan også misbruge billeder i en falsk profil for at opnå en økonomisk gevinst (f.eks. romance scam – se afsnit 3.2.8).

Selvom økonomisk og ærekrænkende misbrug bliver efterforsket i forskellige afdelinger, benytter politiet sig af mere eller mindre de samme efterforskningsmetoder. En politirespondent, som nu er leder af efterforskningen af økonomisk kriminalitet, og som har været leder i en afdeling for almen straffelov, udtrykker det således:

Der har vi de samme efterforskningsmetoder, som vi har i forhold til økonomisk kriminalitet. Hvis det er sådan, at der er efterforskningsmuligheder, så forfølger vi selvfølgelig sagerne. Vi kontakter de pågældende internetsider og hører, hvem ejeren bag den her profil er. Hvad er der af oplysninger på den, som har bragt billederne osv. Det er min vurdering, at det er lidt omstændeligt i forhold til samarbejdet med internetsiderne, men det kan lade sig gøre. Det kan være svært at få større selskaber i tale.

6.3 Hæftelse for tabet

I offerundersøgelsen Internetkriminalitet 2017 (Kruize, 2018) er økonomisk identitetsmisbrug delt op i 'identitetsmisbrug' og 'kortmisbrug'. Ved begge kategorier hæfter dem, der er udsat for misbrug, for 9 % af det samlede tab. Det betyder, at virksomheder står for 91 % af tabet. Det kan være en finansiell virksomhed, men det er også ofte butikkerne, der sidder tilbage med en ubetalt regning. Markedschefen i Dansk Erhverv skriver i denne sammenhæng:³⁹

Dansk Erhverv har i en årrække arbejdet på at få sat en stopper for identitetstyveri. Det er meget ubehageligt for de borgere, det går ud over, men i de fleste tilfælde lider de ingen økonomisk overlast. Det gør butikkerne til gengæld, for i mange tilfælde ender regningen hos dem.

Også politirespondenter påpeger, at netbutikker plejer at henlægge sagen med det samme, når folk gør indsigelse. En af respondenterne mener, at der er ganske få sager, hvor folk gør

³⁹http://detailfolk.dk/blog/lone_rasmussen_dansk_erhverv/identitetstyveri_koster_butikkerne_penge_og_kalder_p_styrket_indsats.html

indsigelse, mens de faktisk selv har handlet. Han fortsætter med "nogle gange har vi mistanke om, at unge, efter f.eks. en bytur, gør indsigelse, men at det i realiteten har været en kammerat, der har brugt kortet. Det kan være ret belastende for folk, hvis låneudbydere holder fast i deres krav og trækker folk i fogedretten; de føler sig jagtet. Det er typisk med kviklån. De holder mere fast i deres krav".

En respondent, der tilbyder forbrugslån (kviklån), fortæller, at de kræver en tro- og loveerklæring, hvor kunden skriver under på, at det ikke er vedkommende, der har optaget lånet. Herefter kan lånevirkksomheden politianmelde sagen. Deres erfaring er, at den forurettede i 9 ud af 10 tilfælde godt ved, hvem der står bag, og de klarer det for det meste internt. Så længe politiet ikke har fundet frem til, hvem der står bag identitetsmisbruget, bliver den person, hvis oplysninger er blevet brugt, stående som låneoptager. Og det bliver kun ændret, når der foreligger en dom.

Vores procedure er, at vi afventer politiet, og vores eksterne samarbejdspartnere overtager typisk sagen på det tidspunkt og afventer politiets afgørelse. Men for at vi kan skifte skyldner på et lånedokument, skal vi have en dom på, at der er begået en forbrydelse, ellers har vi ikke andet at forholde os til, end at der er brugt et NemID med en personlig kode og et cpr-nummer til at underskrive låneforholdet.

Basisbank, som står bag bl.a. LånLet, har kørt mange sager, hvor låneoptageren påstår, at hans/hendes identitet er blevet misbrugt, i fogedretten. I et interview med direktøren for Basisbank (i oktober 2017) bliver der sagt, at de siden juni 2016 har kørt 191 af den her type af sager i fogedretten og har vundet 188 af dem. Direktøren fortæller: "Langt de fleste (90-95 %) har gjort det selv. De har solgt deres NemID for måske 15.000 kr., og så er der blevet taget et lån på 40.000 kr. Bagmænd har tjent 25.000 kr. pr. lån". Tallet på 191 betragter bankdirektøren som toppen af isbjerget.

Der er garanteret flere end 191, som ikke tør anmelde. Selvom de har begået bedrageri og/eller andet kriminelt, er de i bund og grund også ofre. Det kan være dummebøder, betaling af narkogæld osv. Hvis ikke de anmelder det, så hænger de på det selv. Jeg vil tro, at der måske alene hos os er 2.000 kunder, som har lavet det her. Det vil sige, at 1.800 personer ikke har anmeldt det. Det er måske et højt skøn.

Selvom bankdirektøren ikke afviser, at der er nogle, der kan blive udsat for phishing og på den måde har mistet deres NemID-oplysninger, er langt de fleste ofre selv skyldige, for det er meget svært at svindle med NemID. Der er brug for både nøglekort, cpr-nummer og en personlig kode.

Bankrespondenten peger på, at politiet er tilbøjelige til at sigte dem, der har været vidende om, at der blev optaget lån i deres navn, for hæleri. Det bekræftes af en respondent fra Kø-

benhavns Politi: "Jeg talte her til morgen med en kollega, som har siddet med et rigtigt stort kompleks. Præcis ligesom de her lånesager. Hans holdning er også, at NemID-indehaveren er med i det. Jeg ved også, at der ofte bliver sigtet for hæleri i de her sager".

Vores politirespondenter er klar over, at en borger kan blive franarret sine NemID-oplysninger, men der er forskelle på, hvor meget de tror på, at alle anmeldere har rent mel i posen. En af de mere skeptiske politirespondenter udtrykker sin tvivl:

Typisk sker der det, f.eks. i Express Bank eller i Santander Bank eller andre af de her forbrugs-lånsbanker, at der er en, som opretter et lån på 60.000 kr. Der er måske et krav om, at man skal indsende en lønseddel og årsopgørelse. Dem forfalsker man og indsender, og man skriver under med NemID. Typisk en NemKonto, eftersom man skriver under med NemID. Den, der har fået misbrugt sit NemID, den bankkunde skal have fået stjålet sit NemID med NemID-koden og pågældendes personnummer, som også skal være stjålet, så man kan logge ind med NemID. Herefter skal en anden person optage et lån, og pengene skal indgå på NemID-indehaverens konto. Så skal gerningsmanden logge ind på netbank og videreføre pengene. Dette er efter min opfattelse ikke noget, der sker. Det sker ikke uden NemID-indehaverens vidende. Det kan selvfølgelig være, at man er blevet presset til at udlevere det. Det kan også være, man har fået penge for at udlevere det.

6.4 Sletning

I afsnit 5.2.4 har vi beskrevet erfaringer fra udsatte for ærekrænkende identitetsmisbrug med sletning af profiler og billeder. Her ser vi nærmere på, hvordan en profil på Facebook og Instagram kan lukkes, og hvordan man kan fjerne indekseret indhold fra Google. Vi ville gerne have hørt fra Facebook om, hvor ofte de lukker falske profiler i Danmark, og hvor meget indhold Google fjerner, men som beskrevet i afsnit 2.2 har det ikke være muligt at komme i kontakt med disse virksomheder. På Facebooks, Instagrams og Googles hjemmesider kan man læse, hvilket indhold der kommer i betragtning til sletning.

Facebook

Hvis du har en Facebook-konto og gerne vil anmelde en person, der udgiver sig for at være dig eller en anden, du kender: Gå til profilen for den konto, der giver sig ud for at være en anden. Hvis du ikke kan finde profilen, kan du prøve at søge efter det navn, der bruges på den, eller bede dine venner om at sende et link til den. Klik på ... på coverbilledet, og vælg Anmeld. Følg vejledningen på skærmen for identitetstyveri for at indsende en anmeldelse. Hvis du ikke har en Facebook-konto og gerne vil anmelde en person, der udgiver sig for at være dig eller en anden, du kender, skal du udfylde denne formular ([link](#)).

Instagram

Instagram tager sikkerheden alvorligt. Hvis nogen har oprettet en Instagram-konto, der giver sig ud for at være dig, kan du anmelde det til os. Sørg for at angive alle de nødvendige oplysninger,

herunder et billede af dit myndighedsudstedte id. Hvis du har en Instagram-konto, kan du anmelde det til os direkte fra app'en. Hvis du ikke har en Instagram-konto, skal du udfylde denne formular (link). Vi svarer kun på anmeldelser, der sendes til os fra den person, der er udsat for identitetstyveri. Hvis en person, du kender, udsættes for identitetstyveri, skal du opfordre den pågældende person til at anmelde det til os.

Google

I maj 2014 fandt en afgørelse fra EU-domstolen (C-131/12, 13. maj 2014), at visse personer har ret til at anmode søgemaskiner om at fjerne bestemte resultater for forespørgsler, som indeholder deres navn, hvis interessen i de viste resultater ikke opvejer personens ret til privatliv. Når du foretager denne type anmodning, forsøger vi at afbalancere den enkelte brugers ret til privatliv med offentlighedens interesse i at få indsigt i og ret til at videregive oplysninger. Når vi skal vurdere din anmodning, vil vi se på, om resultaterne omfatter forældede oplysninger om dig, samt hvorvidt offentligheden har interesse i oplysningerne – vi kan f.eks. vælge at afvise en anmodning om at fjerne visse oplysninger om økonomisk svindel, pligtforsømmelse, straffedomme eller embedsmænds offentlige adfærd.

Du skal have en digital kopi af et identifikationsbevis for at udfylde formularen. Hvis du indsender denne anmodning på vegne af en anden, skal du vedlægge id-oplysninger for denne person.

7 Eksisterende tiltag

Når en person er udsat for misbrug af sine identitetsoplysninger, kan han eller hun søge efter oplysninger om, hvad der skal gøres for at stoppe/begrænse misbruget og forebygge yderligere misbrug. Det findes mange instanser, der ligger inde med gode råd, men Danmarks officielle vejledende instans er Digitaliseringsstyrelsen, og dens råd er tilgængelige på borger.dk.⁴⁰

Når *identitetstyveri* indtastes i søgefunktionen på borger.dk, kommer 10 resultater frem:

1. Hvad er identitetstyveri?
2. Hvordan foregår identitetstyveri?
3. Offer for identitetstyveri.
4. Hvordan undgår jeg identitetstyveri?
5. Spørgsmål og svar om identitetstyveri.
6. Offer for misbrug af kortoplysninger.
7. Privatliv på sociale medier.
8. Sikker Digital Post.
9. Cykeltyveri og anden kriminalitet.
10. Det Centrale Personregister (CPR).

Når der klikkes på *Offer for identitetstyveri*, er det første budskab: "Hvis du opdager, at du er offer for identitetstyveri, er det vigtigt, at du reagerer på det". Der rådes til at melde tyveriet til politiet, at kontakte aftalepartner, f.eks. kreditorer, omgående og eventuelt at kontakte en advokat. Endelig gøres opmærksom på muligheden for et nyt personnummer. Der bliver gjort opmærksom på muligheden for en kreditadvarsel i CPR under rubrikken *læs også*. Vi ser nærmere på muligheden for et nyt personnummer og kreditadvarsel i CPR i afsnit 7.2 og 7.3.

På borger.dk påpeges det – under overskriften *Hvordan undgår jeg identitetstyveri?* – at man skal være påpasselig med personoplysninger i sit affald. "For at undgå identitetstyveri, som skyldes oplysninger fra dit affald, bør personlige oplysninger i breve eller papir fjernes eller skjules, før dokumenterne smides i skraldespanden". Og så skal man være omhyggelig med

⁴⁰ Siden den 31. oktober 2018 findes der også informationsportal sikkerdigital.dk. Erhvervsstyrelsen og Digitaliseringsstyrelsen står bag Sikkerdigital.dk i samarbejde med Center for Cybersikkerhed, Politiet, Datatilsynet, Det Kriminalpræventive Råd og Forbrugerrådet TÆNK.

kortoplysninger og pinkoder. "Kort og pinkoder bør altid holdes adskilt. For at stoppe eventuelt misbrug af dine kortoplysninger, bør du regelmæssigt tjekke dine kontobevægelser".

Under overskriften *Spørgsmål og svar om identitetstyveri* lyder et af spørgsmålene, om man kan forsikre sig mod identitetstyveri, og svaret er 'ja'. Der henvises til ens forsikringsselskab. Vi ser nærmere på, hvad en forsikring mod ID-tyveri omfatter i afsnit 7.4.

Når en person har mistet sin pung med f.eks. et kørekort og/eller sygesikringsbevis, kan han/hun med god grund være bekymret for, om hans eller hendes identitet bliver misbrugt på den ene eller den anden måde. Derfor kunne det være rart, hvis man kunne tjekke, om der er indgået en kreditaftale et eller andet sted, før der kommer rudekuverter i postkassen. Det er selvfølgelig bedst at aktivere en kreditadvarsel på sit personnummer med det samme (se afsnit 7.3), men hvis det ikke er gjort med det samme, eller man vil tjekke kreditaftaler i sit navn alligevel, så kan KreditStatus hos Experian benyttes. Hvis man frygter, at der er oprettet en virksomhed i ens navn, kan Det Centrale Virksomhedsregister (CVR) tjekkes. I afsnit 7.1 ser vi nærmere på disse to muligheder.

Dette kapitel afsluttes (afsnit 7.5) med en gennemgang af eksisterende tiltag, der tilbydes af Non-Governmental Organisations (NGO'er) som Den Sociale Retshjælp, Red Barnet og Dansk Kvindesamfund.

7.1 Er min identitet blevet misbrugt?

På Experians hjemmeside, under kreditstatus (<http://www.experian.dk/kreditstatus/>), forklares det, hvad KreditStatus står for:

KreditStatus giver adgang til et øjebliksbillede af en persons lån og kreditter hos långivere, der er tilsluttet KreditStatus. Adgangen kræver den pågældende persons samtykke og må kun ske til brug for en konkret kreditvurdering. KreditStatus viser data om en låntagers kreditter og giver på den måde både låntager og kreditgiver et overblik over låntagerens økonomi.

En borger kan få et overblik over lån (ikke realkreditlån) i sit navn og på den måde få indblik i, om der er indgået en aftale, han/hun ikke kender til. Ifølge Experian giver KreditStatus indblik i lån og kreditter hos følgende 14 finansvirksomheder:

- Bank Norwegian AS
- Capitolia ApS
- COOP Bank A/S
- CreamFinance Denmark ApS
- Express Bank A/S

- EnterCard Danmark – filial EnterCard Norge AS
- Ikano Bank – filial af Ikano Bank AB (publ), Sverige
- Mozipo ApS
- Nordea Finans Danmark A/S
- Resurs Bank, Filial af Resurs Bank Aktiebolag, Sverige
- Santander Consumer Bank, Filial af Santander Consumer Bank AS, Norge
- SEB Kort Bank, Danmark, Filial Af SEB Kort Bank AB, Sverige
- Spar Nord Bank A/S
- 4finance ApS.

Der kan være indgået en direkte låneaftale med en af disse finansvirksomheder. Hvis der er købt på kredit i en butik, er det for det meste også synligt i KreditStatus, for disse virksomheder står ofte bag den form for kredit. Express Bank samarbejder bl.a. med Elgiganten, Bilka og Jysk, så hvis en forbruger gerne vil købe en vare på kredit hos en af de kæder, er det Express Bank, der står for finansieringen.

Hvis man frygter, at der er oprettet en virksomhed i ens navn, kan det tjekkes ved at indtaste navn, personnummer eller adresse på <https://datacvr.virk.dk/data/>. CVR indeholder oplysninger om alle registrerede virksomheder i Danmark og Grønland, såsom adresse, branche og deltagere.

7.2 Nyt personnummer

I 2014 blev det muligt at anmode om et nyt personnummer i forbindelse med identitetsmisbrug. Folketinget vedtog den 25. marts 2014 en ændring af CPR-loven, og ordlyden af bestemmelsen er således:

Økonomi- og Indenrigsministeriet kan efter skriftlig anmodning herom i særlige tilfælde tildele nyt personnummer til en person, hvis personnummer indgår eller har indgået i forbindelse med misbrug af vedkommendes identitet (CPR-loven, § 3, stk. 7).

I forbindelse med behandlingen af lovforslaget blev det tilsagt, at Økonomi- og Indenrigsministeriet vil udarbejde en årlig opgørelse over antallet af ansøgninger om, tildelinger af og afslag på anmodninger om nyt personnummer. Opgørelsen vil også indeholde en redegørelse for begrundelsen i den enkelte sag for tildeling af nyt personnummer, henholdsvis afslag herpå.

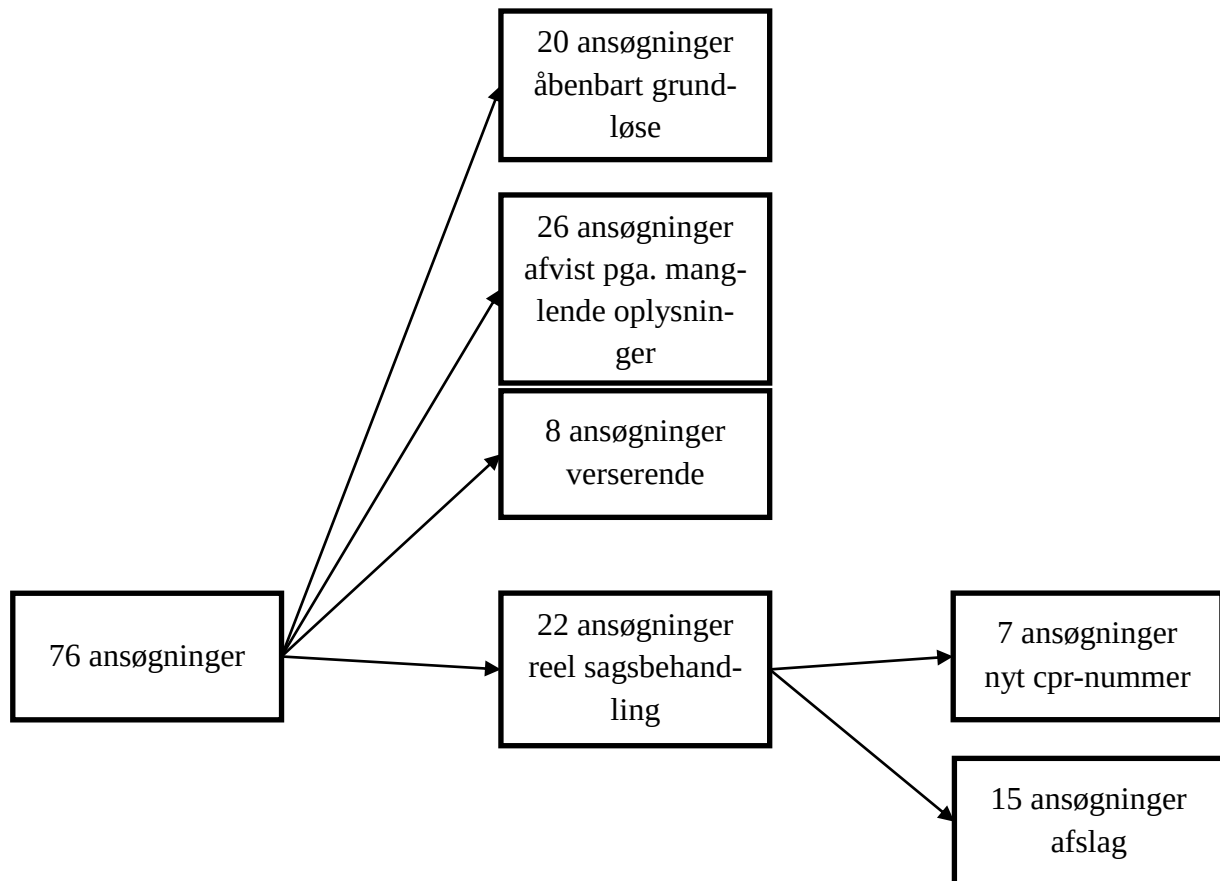
Der er i skrivende stund sendt fire opgørelser til Folketinget. Opgørelsesperioden løber fra d. 1. april til og med d. 31. marts. De fire opgørelser omhandler årene 2014/2015, 2015/2016, 2016/2017 og 2017/2018. I den første periode er der indsendt 29 ansøgninger, i de tre efter-

følgende perioder henholdsvis 14, 13 og 20 ansøgninger, altså i alt 76 ansøgninger. I opgørelserne skelnes mellem fire afgørelsestyper:

1. Åbenbart grundløs: Grundlaget for betegnelsen åbenbart grundløs er, ifølge ministeriets redegørelse, meget forskelligt. Det kan være offentliggørelse af personnummeret, uden at der er konstateret et misbrug i den forbindelse, at pågældende frygter for sit liv på grund af vidneudsagn i en straffesag eller konspirationsagtige historier (aflytning af politiet, spionage eller chikane fra politiet/pengeinstitut). Hvis sagen betragtes som åbenbart grundløs, informeres ansøgeren om indholdet af reglerne, og det meddeles ansøgeren, at ministeriet på det foreliggende grundlag må afvise anmodningen om et nyt personnummer.
2. Manglende oplysninger: Ansøgeren skal indsende dokumentation for misbruget af sit cpr-nummer, typisk politianmeldelse og brevveksling med virksomheder og myndigheder. Hvis dette mangler eller er mangelfuldt, finder der ingen sagsbehandling sted. Ministeriet tilkendegiver over for ansøgeren, at sagen kun behandles, hvis de nødvendige dokumenter bliver tilsendt.
3. Nyt cpr-nummer: På baggrund af den indgivne ansøgning og yderligere indhentede oplysninger er der tildelt et nyt personnummer.
4. Afslag: På baggrund af den indgivne ansøgning og yderligere indhentede oplysninger er der ikke tildelt et nyt personnummer.

Figur 7.1 viser, at kun en fjerdedel – 22 af de 76 ansøgninger – opfylder kravene for en reel sagsbehandling. De andre ansøgninger er åbenbart grundløse, eller der mangler oplysninger. Otte sager er ikke afgjort endnu. Syv ansøgere har fået tildelt et nyt cpr-nummer.

Figur 7.1: Afgørelse på 76 ansøgninger om nyt personnummer (april 2014-marts 2018)



Kilde: Økonomi- og Indenrigsministeriet; egne beregninger

I Økonomi- og Indenrigsministeriets opgørelse for 2014/2015 og 2015/2016 beskrives sager, i hvilke anmodning om et nyt cpr-nummer har ført til en reel sagsbehandling. I de sidste to opgørelser mangler denne beskrivelse. Der har været en reel sagsbehandling i fem sager i både 2014/2015 og 2015/2016; i alt ti sager. I alle sager er ansøgerens personnummer blevet misbrugt. I tre sager har gerningspersonen ikke kun fået adgang til ansøgerens personnummer, men der er også stjålet identitetsdokumenter (kørekort, sundhedskort, pas). I tre andre sager er der tale om et familiært bånd mellem ansøger og gerningsmand (fætter, tidligere ægtefælle og forælder).

I sager, hvor ansøger har fået tildelt et nyt personnummer, bliver der lagt vægt på, at misbrug er sket i flere omgange, at misbruget har et vist omfang, og at det har påvirket ansøgeren psykisk. I de sager, hvor der er givet afslag på ansøgningen, er der lagt vægt på, at misbruget er ophørt, efter at en gerningsmand er blevet sigtet i sagen. Afslag er også givet i sager, hvor

ministeriet tvivler på, at personnummeret har været afgørende for misbruget. Det gælder f.eks. i en sag om chikane begået af en tidligere ægtefælle.

7.3 Kreditadvarsel i CPR

I 2017 er det blevet muligt at få indsat en markering i CPR om, at borgeren ønsker at advare mod kreditgivning i vedkommendes navn. Folketinget vedtog den 1. december 2016 en ændring af CPR-loven, og ordlyden i bestemmelsen er, som følger:

Enhver, der er fyldt 15 år, har ret til ved henvendelse til sin bopælskommune at få indsat en markering i CPR om, at vedkommende ønsker at advare mod kreditgivning i vedkommendes navn, med henblik på at oplysning herom fra CPR kan videregives til offentlige myndigheder og private i overensstemmelse med §§ 31, 32, 38, 39 og 42. (CPR-loven, § 29, stk. 3).

Det er en frivillig ordning. I bemærkningerne til lovforslaget påpeges det, at bestemmelsen giver enhver borger (som er fyldt 15 år) mulighed for at advare mod kreditgivning i vedkommendes navn. Det kan være, at borgeren er bekymret for identitetsmisbrug, efter at vedkommende har mistet sine personlige identifikationsdokumenter, eller at borgeren har været udsat for identitetsmisbrug. I begge tilfælde kan det være relevant at gøre lån- og kreditgivere opmærksomme på, at disse ikke umiddelbart skal yde lån eller kredit til personer, der udgiver sig for at være den pågældende. I bemærkningen til lovforslaget gøres også opmærksom på, at ordningen også er til gavn for virksomhederne. De hæfter som regel for det økonomiske tab i forbindelse med identitetsmisbrug.

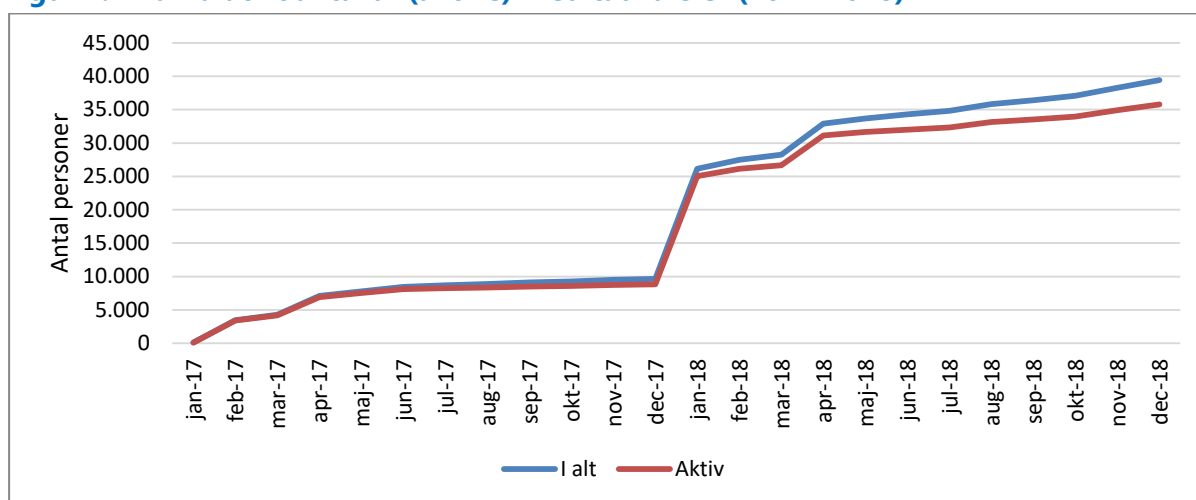
En borger kan selv indsætte en kreditadvarsel på sit personnummer på borger.dk. Der skal logges ind med NemID. Her kan advarslen også ophæves. Der gøres opmærksom på, at en kreditadvarsel kan spærre for pågældendes egne muligheder for at opnå lån eller kredit. I givet fald kan advarslen (midlertidigt) ophæves.

Oplysninger fra CPR-kontoret viser, at muligheden for kreditadvarsel i CPR benyttes af et betydeligt antal borgere. Tallene viser ikke baggrunden for markeringen: Er formålet præventivt, f.eks. fordi den pågældende har tabt eller fået stjålet identitetsoplysninger/dokumenter, eller er det som følge af oplevet identitetsmisbrug?

Ved udgangen af 2018 har 39.439 personer benyttet sig af en kreditadvarsel i CPR. Ved 35.769 personer er advarslen stadig aktiv pr. 31. december 2018. Det betyder, at 3.670 borgere har ophævet kreditadvarslen. Det svarer til 9,3 % i en periode på to år (fra januar 2017 til og med december 2018).

Figur 7.2 viser det kumulative antal borgere, der har benyttet sig af en kreditadvarsel i perioden januar 2017 til og med december 2018, og det kumulative antal aktive advarsler. Den markante vækst i antallet af kreditadvarsler i januar 2018 er iøjnefaldende. Ifølge en repræsentant for Økonomi- og Indenrigsministeriet skyldes denne vækst en række udsendelser om identitetstyveri på alle Danmarks Radios platforme (web, radio, TV). I disse indslag udpeges kreditadvarsel som et redskab til at komme identitetsmisbrug til livs. Kreditadvarsel bliver i disse indslag rost af Økonomi- og indenrigsministeren, den operative chef for Rigspolitiets Cyber Crime Center (NC3), direktøren i Finans og Leasing og kommunikationschefen i Express Bank.⁴¹

Figur 7.2 Kumulativt antal af (aktive) kreditadvarsler (2017-2018)



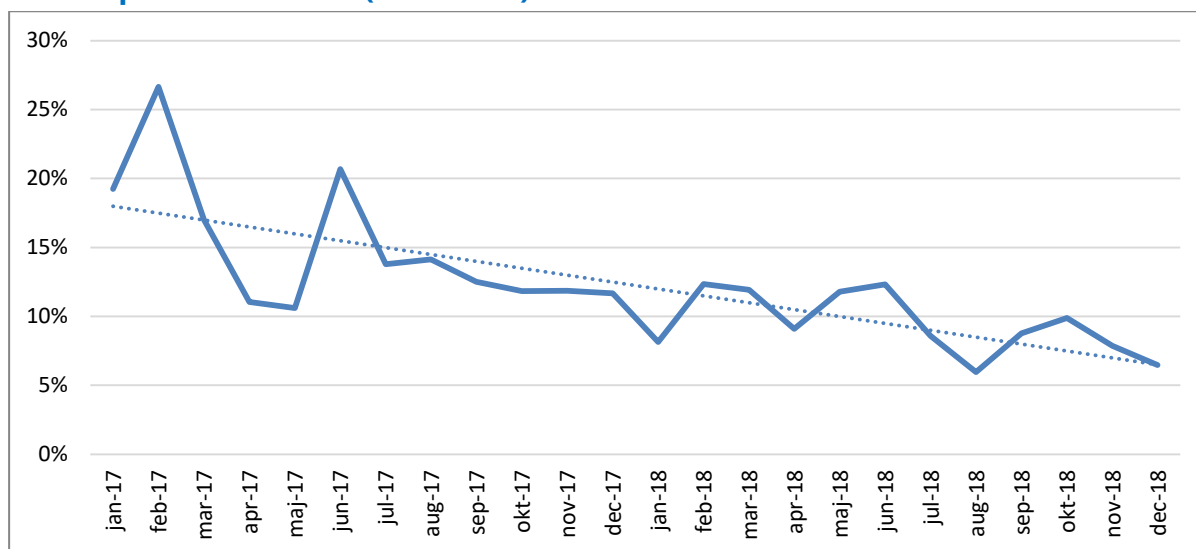
Kilde: Data fra CPR-kontoret; egne beregninger

Det forekommer, at borgere midlertidigt ophæver deres advarsel – formentlig fordi de selv har brug for kredit – og efterfølgende aktiverer advarslen igen. Dette gælder for 1.543 personer.

I gennemsnit er 9,3 % af kreditadvarslerne blevet ophævet, det vil sige, at advarslen ikke var aktiv i december 2018. Sandsynligheden for, at en borger ophæver advarslen, øges, jo længere advarslen har været aktiv. Sagt på en anden måde: Sandsynligheden for, at en person, der har aktiveret advarslen i februar 2017, har ophævet den igen før december 2018, er større end sandsynligheden for, at en person, der har aktiveret advarslen i november 2018, allerede har ophævet advarslen i december 2018. Figur 7.3 bekræfter denne tankegang.

⁴¹ Se: <https://www.dr.dk/nyheder/indland/tusindvis-af-danskere-bruger-nyt-forsvar-i-kampen-mod-identitetstyve>

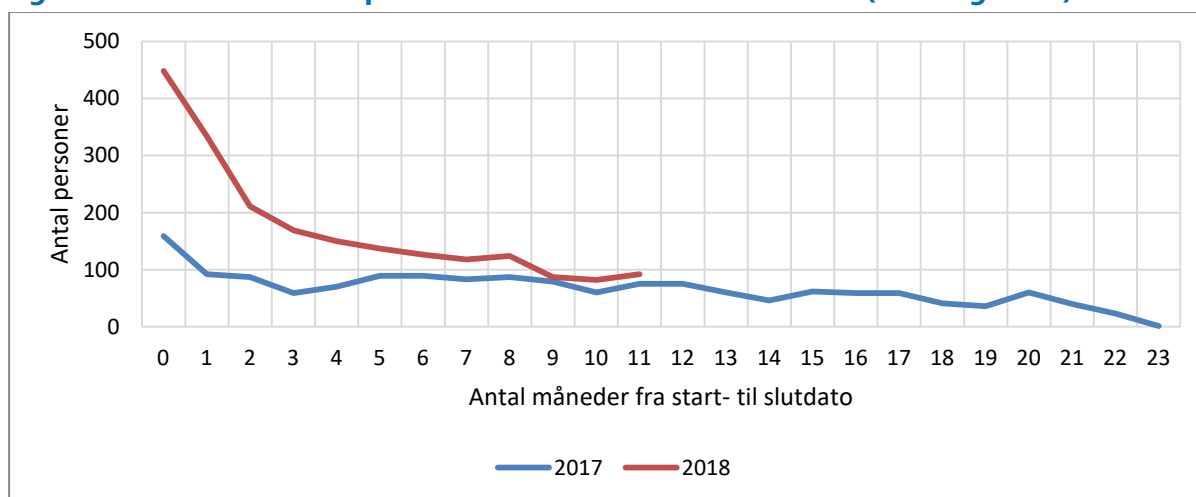
Figur 7.3 Andelen af borgere, der har ophævet kreditadvarslen, opgjort efter hvornår de har oprettet advarslen (2017-2018)



Kilde: Data fra CPR-kontoret; egne beregninger

Figur 7.4 viser, hvor mange måneder der er gået, før en person ophæver kreditadvarslen igen. 22 % af dem, der har sat en advarsel på deres personnummer og ophævet den igen i 2018, har gjort det inden for den samme måned. Det gælder kun for 10 % af dem, der har sat en advarsel på deres personnummer i 2017 og efterfølgende ophævet den i 2017 eller 2018. Denne forskel skyldes – i hvert fald delvist – at perioden for at ophæve advarslen er længere for dem, der har aktiveret advarslen i 2017, end for dem, der har gjort det i 2018.

Figur 7.4 Antal måneder ophævede advarsler har været aktive (2017 og 2018)

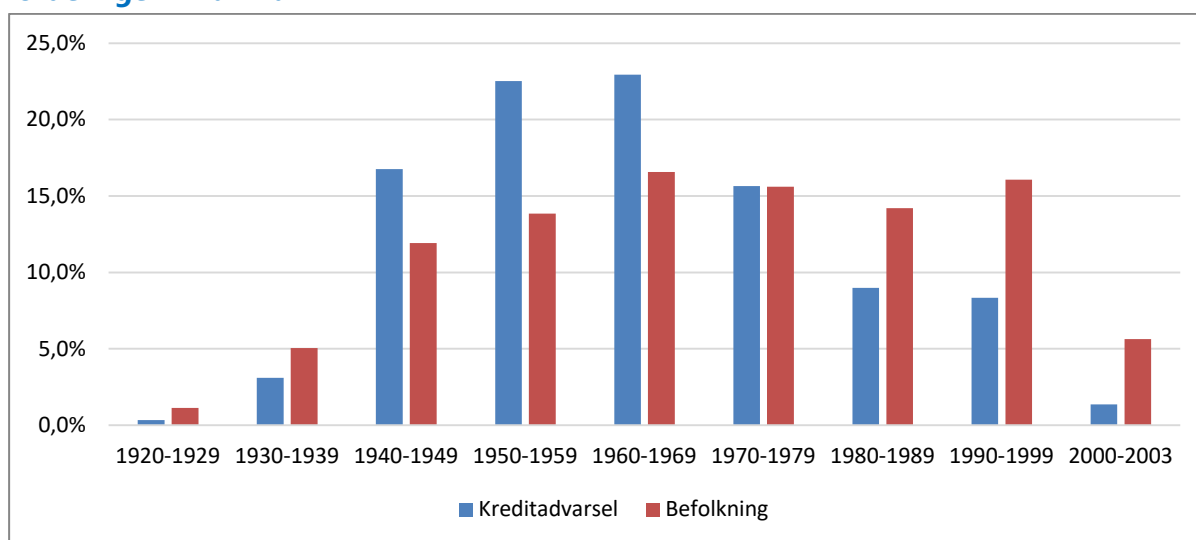


Kilde: Data fra CPR-kontoret; egne beregninger

CPR-kontorets datasæt indeholder også oplysninger om køn og fødselsår hos dem, der har sat en kreditadvarsel på deres personnummer. Kønsfordelingen er tæt på 50-50. Mænd står for 52 % af dem med en kreditadvarsel, mens kvinder tegner for 48 %.

Figur 7.5 viser resultatet af alderen (fødselsår). Der er ikke kun set på, hvilken andel en aldersgruppe har i forhold til kreditadvarsler, men også på deres andel i befolkningsstatistikken. På den måde bliver det påvist, at dem, der er født i 1940'erne, 1950'erne og 1960'erne, er overrepræsenterede blandt dem, der har benyttet sig af en kreditadvarsel i CPR. Det vil sige borgere, der er over 50 år gamle. Det er formentlig ikke et udtryk for, at de har en større risiko for, at deres personoplysninger bliver misbrugt, men at de er mere risikobevidste, og at de hyppigere benytter sig af dette forebyggende tiltag.

Figur 7.5 Fordelingen af kreditadvarsler i CPR efter fødselsår i forhold til befolkningsfordelingen i Danmark



Kilder: Data fra CPR-kontoret (kreditadvarsel) og Statistikbanken (befolkning); egne beregninger

7.4 Forsikring mod identitetstyveri

Langt de fleste forsikringsselskaber dækker identitetstyveri i deres familieforsikring. Langt de fleste danskere er dermed forsikret mod ID-tyveri, men det er uvist, hvor mange der er klar over det. Vi har ikke set på forsikringsbetingelserne hos alle selskaber, men hos følgende seks selskaber, som dækker den største del af det danske forsikringsmarked⁴²:

- Tryg (markedsandel 18,1 %)
- Topdanmark (markedsandel 17,4 %)
- Codan (markedsandel 11,3 %)
- Alm. Brand (markedsandel 9,7 %)
- Gjensidige (markedsandel 6,5 %)
- Alka (markedsandel 4,1 %).

⁴² Se: <https://www.forsikringsportalen.dk/forsikringsselskaber/20-stoerste-forsikringsselskaber/>

7.4.1 Økonomisk misbrug

Det er iøjnefaldende, at de seks forsikringsselskaber langt hen ad vejen har defineret identitetstyveri på samme måde. Tryg, Alm. Brand og Gjensidige betragter følgende som identitetstyveri:

Ved identitetstyveri forstås situationer, hvor din/dine identitets-/ identifikationspapirer, uden samtykke fra dig, uberettiget bliver brugt af en anden/andre person(er) med henblik på økonomisk vinding, som f.eks. i dit navn at åbne kreditkonto, søge om lån, registrere telefonabonnementer, køb af varer mv.

Ved identifikationspapirer forstås enhver legitimation, som er egnet til at identificere dig, f.eks. pas, bankkort, kørekort, cpr-nummer, kontonummer, login-kode, brugernavn/adgangskode til internettjenester, elektronisk signatur, NemID, lønseddel og andet tilsvarende materiale.

Topdanmark, Codan og Alka definerer identitetstyveri, som følger:

Ved identitetstyveri forstås vi ulovlig eller uautoriseret brug af dine identifikationspapirer med henblik på økonomisk vinding fra tredjepart.

Ved identifikationspapirer forstås vi dokumenter, som bekræfter din identitet, f.eks. pas, kørekort, bankkort, brugernavn/adgangskode til internettjenester, elektronisk signatur, NemID, lønseddel, udbetalingsanvisning og andet materiale, som er egnet til at identificere dig.

Identitetstyveri kan være:

- Lån optaget i dit navn f.eks. ved hjælp af stjålet sundhedskort
- Kreditkonto åbnet med f.eks. et stjålet eller forfalsket pas som dokumentation
- Abonnementer oprettet i dit navn ved hjælp af dit cpr-nummer.

Topdanmark, Codan og Alka gør også klart, hvad der *ikke* betragtes som identitetstyveri. Selvom Tryg, Alm. Brand og Gjensidige ikke skriver det samme i deres betingelser, må vi antage, at de heller ikke anser følgende tilfælde som værende identitetstyveri:

- Betaling med stjalne betalingskort
- Misbrug af identitet på sociale medier
- Tyveri fra bankkonto ved brug af kontooplysninger, som du f.eks. er blevet franarret ved phishing, hvor personer eller firmaer ved falske e-mails, hjemmesider eller telefonopkald får udleveret kontooplysninger.

Alle seks forsikringsselskaber tilbyder rådgivning og hjælp med at skabe overblik og vil hjælpe med at tage kontakt til kreditorer og gøre indsigelse. Forsikringen dækker *ikke* omkostninger og/eller økonomisk tab. Forsikringen kan ikke anvendes, hvis identitetstyveriet er ud-

ført af en eller flere af den sikredes husstand, eller hvis identitetstyveriet kan relateres til arbejde eller beskæftigelse.

Udover rådgivning og hjælp til at skabe overblik og tage kontakt til kreditorer åbner forsikringen hos fire af de seks selskaber for juridisk bistand. Tryg og Gjensidige har begrænset juridisk bistand til maks. 25.000 kr. Codan sætter også beløbsgrænsen til 25.000 kr. eller 10 timers juridisk bistand. Hos Alm. Brand er juridisk bistand begrænset til maks. 20 timer.

Flere af forsikringsselskaberne yder ikke selv bistand til udsatte for identitetstyveri, der henvender sig til deres forsikringsselskab, men har udliciteret denne opgave til Affinion.

I en nordisk undersøgelse af Novus (for Affinion International) er 1.031 danskere i juni 2017 bl.a. blevet spurgt om, hvorvidt de er bekendt med 'any services and/or companies', der kan tilbyde en eller anden form for hjælp ved økonomisk misbrug af deres identitet. 80 % af de adspurgte svarede, at de ikke har kendskab til det. Det tyder på, at langt de fleste borgere ikke er klar over, at de kan henvende sig til deres forsikringsselskab, hvis de har brug for rådgivning, vejledning eller hjælp til at få styr på kreditorerne.

I 2015 og 2016 modtog Affinion Danmark 500 til 600 henvendelser årligt i forbindelse med identitetsmisbrug. Langt de fleste henvendelser var fra personer, der havde mistet deres identitetsoplysninger og ville høre, hvad de så skulle gøre, eller som henvendte sig for at høre, hvad de kunne gøre for at begrænse risikoen for at blive udsat for identitetsmisbrug. I 2015 modtog Affinion Danmark 61 henvendelser, der krævede handling for at begrænse skaderne som følge af identitetsmisbrug. I 2016 var dette antal nået op på 73, og de første fem måneder af 2017 tyder på, at 2017 ender på nogenlunde det samme niveau som 2016.

Affinion skriver i sin ID-sikringspamflet: "Hvis det viser sig, at kunden har været udsat for identitetstyveri og ønsker vores hjælp til at håndtere sagen og hjælpe med at afvise uretmæssige betalingskrav, skal kunden give Affinion en fuldmagt til at indhente oplysninger eller iværksætte tiltag på kundens vegne". For at få indblik i, hvordan sådan en hjælpende hånd fungerer i praksis, har Affinion beskrevet sagsforløbet i to sager.

En typisk ID-sag

Klaus er 25 år gammel og henvender sig i starten af maj. For 14 dage siden fik han stjålet sin pung med betalingskort, kørekort, sygesikringsbevis, studiekort og rejsekort. Han fik alt spærret og politianmeldt med det samme. Der blev alligevel købt fem iPhones i hans navn ved fire forskellige teleselskaber (Telenor, YouSee, Telia og Hi3G). I forbindelse med køb i YouSee er der oprettet lån ved Express Bank.

Klaus giver en fuldmagt, og der sendes en indsigelse til alle kreditorer sammen med en kopi af politianmeldelsen. Efterfølgende modtager Klaus Tro og Love-erklæringer fra alle kreditorer, som udfyldes og returneres. De fleste kreditorer sletter kravene, men Telenor og Express Bank

har sat deres krav i bero og afventer politiets sagsbehandling. Ifølge loven må kreditorerne ikke sende rykkere med gebyr i en tvistsag, men Klaus modtager alligevel en del rykkere. Det er typisk en systemfejl (rykkeren sendes automatisk), og Klaus skal se bort fra disse. Alligevel er det belastende at modtage regning efter regning.

Kreditor vil indgå forlig

Jens har været på ferie, og når han kommer hjem, ligger der et inkassobrev på 3.000 kr. Jens har ikke handlet der, hvor inkassobrevet henviser til. Efterfølgende modtager han en regning fra Hi3G for køb af en iPhone plus abonnement. Han har selv kontaktet Hi3G og får tilsendt en Tro og Love-erklæring, som han udfylder og sender retur. Af købsaftalen fremgår det, at der er brugt cpr-nummer til købet. Købet er gjort telefonisk, og aftalen er sendt til en Gmail-adresse oprettet i Jens' navn.

Hi3G svarer, at de mener, at beviserne mod Jens er stærke, og tilbyder et forlig. Det består i, at abonnementet bliver slettet, men iPhone skal betales kontant. Forligsforslaget afvises. Post Danmark, som har udleveret pakken, kontaktes med spørgsmål om, hvorvidt der er beviser for, at Jens modtog pakken. Ifølge Post Danmarks egne regler for udlevering skal postbuddet se, at den pågældende går ind i huset/lejligheden eller åbner døren indefra. Disse krav er ikke overholdt. Post Danmark sender en kopi af den falske underskrift. Med underskriften fremgår der også tidspunktet for udlevering – kl. 11.31. På Jens' arbejdsplads er han registreret for et salg kl. 11.43, og han arbejder 45 minutter fra sit hjem. Med disse oplysninger frafalder Hi3G alle krav.

7.4.2 Ærekrænkende misbrug

Der er flere forsikringsselskaber, der tilbyder hjælp ved misbrug eller chikane på sociale medier. Hos Tryg er det en del af Tryg ID. Codan reklamerer med Websikring, som de tilbyder gratis og uden binding i 2019 for deres kunder. Ligesom ved økonomisk misbrug benytter disse forsikringsselskaber sig af Affinion til at varetage disse ydelser. Affinion kalder denne form for støtte for Web Cleanup.

Web Cleanup tilbyder hjælp i bl.a. følgende situationer:

- Uønskede og/eller krænkende billeder og videoer
- Krænkende kommentarer og trusler
- Hackede brugerkonti og e-mailkonti
- Møbning og anden chikane
- Falske profiler på sociale medier
- Personlig information, som er spredt ulovligt.

Desuden kan man tage kontakt til Affinions agenter for at få rådgivning om god netadfærd og om, hvordan man får kontrol med og overblik over sit barns adfærd på nettet.

Også her skal kunden give en fuldmagt til Affinion. De kan så, om ønsket, kontakte websteder, hvor det uønskede indhold ligger, for at fjerne oplysningerne. Forudsætningen er dog, at indholdet er i strid med webstedets brugsbetingelser og/eller er i strid med gældende (dansk) ret.

Som beskrevet i afsnit 5.2.4 er det ikke altid nemt at fjerne indholdet fra nettet. Affinion har beskrevet et forløb med at fjerne billeder fra nettet.

Preggo porn

Sara og Emil er forældre til tvillinger. Sara har under graviditeten søgt råd og vejledning på hjemmesider for gravide og i flere Facebook-grupper. En af disse grupper er rettet mod tvillingemødre. En dag får Sara at vide, at hendes billede er blevet brugt af en anden kvinde – og den kvinde skriver, at hun skal føde i morgen.

Sara beder om råd til, hvordan hun skal forholde sig til det. Hun rådes til at anmelde denne brugerprofil og billedet og spørger om, hvorvidt andre brugere af gruppen vil bakke hende op. Administratoren kan efterfølgende udelukke denne kvinde fra gruppen. Eftersom billedet er postet i en lukket gruppe, kan det dog ikke fjernes.

Sara bliver bedt om en kopi af billedet, og efterfølgende gennemføres en billedsøgning på nettet. Det viser sig, at Saras billede ligger på flere forskellige 'preggo porn'-sites. Diverse sider anmodes om at fjerne billedet. Det lykkes at få fjernet billedet fra de fleste sider, dog ikke fra Tumblr.⁴³ I stedet laves en afindeksering i Google. Men Sara har opdaget, at billederne bliver brugt igen, og i to omgange får hun hjælp til at fjerne billedet fra adskillige pornosider.

7.5 NGO'er

Der er flere NGO'er, der tilbyder hjælp til udsatte for (en form for) identitetsmisbrug. Forbrugerrådet Tænk har udviklet en app – Mit Digitale Selvforsvar – som bl.a. holder dem, der har downloadet denne app, opdateret om fupmails i omløb, falske konkurrencer, digital svindel eller registrerede trusler fra vira og skadelig software. Sker skaden, vejleder app'en med konkrete råd til at løse problemet. Den Sociale Rets hjælps Fond giver en hjælpende hånd til socialt udsatte, der er blevet ofre for identitetsmisbrug. Desuden er der to NGO'er, der hjælper med sletning af krænkende billeder på internettet: Dansk Kvindesamfund hjælper voksne, der er blevet udsat for krænkende billeddeling, mens Red Barnet yder hjælp til børn.

7.5.1 Mit Digitale Selvforsvar (Forbrugerrådet Tænk)

App'en har fire funktioner: Guides, Advarsler, Artikler og Tip os. Under Guides ligger, som navnet lægger op til, et antal guides med "konkrete råd og tips, der hjælper dig til en trygge digital hverdag". Og så er der en 'førstehjælpskasse' med navnet "Når skaden er sket". Når

⁴³ Tumblr bruges til at dele flere forskellige slags medier, heriblandt billeder og lydfiler. Det er herudover også muligt at følge og kommentere andre brugeres opslag.

man klikker på førstehjælpskassen, får man spørgsmålet 'Hvad er der sket?' Der findes følgende svarmuligheder:

1. Jeg har videregivet mine kortoplysninger.
2. Jeg har videregivet mine NemID-oplysninger.
3. Jeg har deltaget i en fup-konkurrence.
4. Jeg har handlet i en fup-butik på nettet.
5. Jeg har ringet tilbage til et fup-telefonnummer.
6. Jeg er blevet udsat for identitetstyveri.
7. Min e-mailkonto er blevet hacket.
8. Mine filer er blevet låst af en hacker.
9. Jeg har fået delt et nøgenbillede.

Alle disse kategorier – på nær 'Mine filer er blevet låst af en hacker' (ransomware) – kan være relevante i forbindelse med identitetsmisbrug. De første seks kategorier kan være et led i økonomisk identitetsmisbrug. Identitetstyveri er her defineret som 'Modtager du regninger for varer, du aldrig har købt? Eller lån, du aldrig har oprettet?' Der bliver for det meste givet vejledning i tre trin, og det samme råd gives i forskellige situationer. Nedenstående skema viser de syv råd, der gives for de seks nævnte situationer. Et nummer i skemaet betyder for det første, at dette råd er givet i den korresponderende situation, og henviser for det andet til rækkefølgen. Hvis en person har videregivet sine NemID-oplysninger, gives følgende råd:

1. Spær NemID.
2. Anmeld til politiet.
3. Slet og bloker (phishing e-mail/sms).

Råd efter at skaden er sket (Mit Digitale Selvforsvar)

		Spær kort/ NemID	Indsigelse	Slet og bloker	Kontakt firma	Anmeld til politiet	Anmeld til tele-selskab	Kredit-advarsel
1	Kortoplysninger	1	2	3				
2	NemID	1		3		2		
3	Fup-konkurrence	1	2		3			
4	Fup-butik	1	3		2	4		
5	Fup-telefonnummer			1			2	
6	ID-tyveri				1	2		3

Hvis en persons e-mailkonto er blevet hacket, så rådes til følgende: 1. skift adgangskode, 2. gendan kontoen og 3. rens computer eller telefon. Ved deling af et nøgenbillede er opskriften: 1. begræns spredning, 2. anmeldt til politiet og 3. søg råd og vejledning. Ved det sidste punkt henvises til Red Barnet, hvis det drejer sig om et barn under 18 år.

7.5.2 Den Sociale Retshjælps Fond

En respondent fra Den Sociale Retshjælps Fond (DSRF) skønner, at de har ca. 50-100 identitetsmisbrugssager om året. Ca. 75 % af disse misbrugssager relaterer sig til gademiljøet. Når en person henvender sig til DSRF, vejledes vedkommende om sin retsstilling og sine muligheder. Ifølge respondenterne siger de fleste personer, der har henvendt sig, at 'det er lige meget'. Rådgivningen er også mest teoretisk, for ofrene kan alligevel ikke betale den gæld, der er stiftet i deres navn; de er på kontanthjælp.

Sagen bliver besværlig, hvis misbrugeren har fået fat i udsattes NemID-oplysninger, for så er det svært at løfte bevisbyrden. Og, fortsætter respondenterne fra DSRF, så er det hurtigt groft uagtsomt, for offeret har udleveret sin NemID-kode og sit nøglekort.⁴⁴ Det sker i gademiljøet, men også i parforhold. En gang imellem ender en sag i fogedretten, men det er sjældent. For at anke en sag til landsretten, kræves en forsikring. DSRF må ikke føre en sag i landsretten. Den skal føres af en advokat.

7.5.3 StopChikane (Dansk Kvindesamfund)

StopChikane er et tilbud til voksne, der er eller har været udsat for digitale billedkrænkelser. Alle over 18 år kan kontakte StopChikane, uanset køn, alder (dog over 18 år) og seksuel orientering. Unge/børn under 18 år henvises til Red Barnet. Der ydes gratis rådgivning i, hvordan man dokumenterer billeddelingen, hvordan og hvornår det kan anmeldes til politiet, og hvordan man håndterer konsekvenserne og stopper yderligere deling.

StopChikane kan kontaktes pr. telefon (telefonen er åben 4 timer om ugen) eller pr. e-mail. Ellers ligger der vejledninger på nettet (<https://krisecentrene.dk/stopchikane/vejledninger/>) i forhold til:

- **Dokumentation.** Hvis du bliver udsat for digitale billedkrænkelser, er det vigtigt, at du dokumenterer hele forløbet til brug for anmeldelse og en evt. retssag. Vejledningen går ud på, hvordan man kan tage et screenshot.

⁴⁴ Denne påstand bliver bekræftet af en højesteretskendelse (Sag 82/2018 og 87/2018): "A og B udleverede deres nøglekort til Nem-ID sammen med brugernavn og adgangskode til tredjemænd, som herefter optog lån hos Basisbank A/S. Højesteret udtalte, at afgørelsen (...) må træffes på grundlag af en konkret vurdering af det samlede hændelsesforløb. I denne vurdering indgår bl.a., under hvilke omstændigheder tredjemand er kommet i besiddelse af indehaverens nøgle (brugernavn, adgangskode og nøglekort til Nem-ID), om indehaveren har haft kendskab til, at tredjemand er kommet i besiddelse af de pågældende oplysninger, og om indehaveren har gjort, hvad der var muligt for at forhindre misbrug, f.eks. ved at spærre sit Nem-ID så hurtigt som muligt. A og B havde udvist en sådan grad af uagtsomhed, at de i forhold til Basisbank hæftede for låne-optagelserne på aftaleretligt grundlag, selv om underskrifterne ikke var tilføjet digitalt af dem selv."

- **Stop spredningen.** Hvis dine billeder er blevet spredt via sociale medier, kan du selv gå ind at slette billeder, anmelde og fjerne tags. Vejledningen går ud på, hvordan man fjerner tags fra Facebook, sletter og anmelder billeder/videoer på adskillige sociale medier (Instagram, YouTube, SnapChat, Tumblr, WhatsApp), og hvordan man sletter en Skype-konto.
- **Politianmeldelse.** Vi anbefaler alle, som er udsat for digitale billedkrænkelser, at anmelde det til politiet. Og så henvises der til en vejledning i, hvordan man anmelder en seksualforbrydelse på politi.dk (<https://krisecentrene.dk/wp-content/uploads/politianmeldelse-1.pdf>).
- **Luk ned for chikane på telefon.** Oplever du chikane i form af uønskede opkald fra fremmede personer, kan du lukke din telefon ned for disse. Der er lidt forskel på, hvordan man gør på forskellige telefoner. Der findes en vejledning for en iPhone og en Huawei-telefon.
- **GPS og lokationstjenester.** Hvis du ikke ønsker, at andre skal kunne finde dig fysisk igennem din telefon, skal du slå GPS og lokationstjenester fra. Dette kan man bl.a. gøre på sin iPhone og WhatsApp. Vær opmærksom på, at også andre apps kan indeholde GPS.

7.5.4 SletDet (Red Barnet)

SletDet er 'børnevarianten' af StopChikane, men er ikke kun rettet mod billeddeling. SletDet hjælper også med at få slettet profiler og privat information. Udover hjælp til sletning kan rådgiverne støtte børn i den måske svære situation, de står i. SletDet kan kontaktes pr. telefon (telefonen er åben 4 timer om ugen) eller pr. e-mail. På hjemmesiden gøres barnet bekendt med, at henvendelsen er fortrolig, og at rådgiverne har tavshedspligt. Barnet bliver på hjemmesiden også forberedt på, hvad der vil blive spurgt om, hvis han eller hun ringer:

Når du ringer til os, spørger vi dig om forskellige ting. Det er helt ok, hvis der er nogle af spørgsmålene, du ikke kan svare på. For at vi kan hjælpe dig bedst muligt, er det vigtigt, at du fortæller os så meget som muligt. Når du ringer, spørger vi dig om:

- Hvad er blevet delt? Informationer? Billeder/videoer?
- Hvad viser det?
- Hvem har delt det?
- Hvor og hvordan er det blevet delt? Over mobilen? På Facebook? Andre steder?
- Hvem og hvor mange tror du har set det?

Nogle gange kan vi have brug for tid til at undersøge, hvordan vi kan hjælpe dig bedst muligt. Derfor kan det være, at vi spørger efter dit telefonnummer eller din e-mailadresse, så vi kan kontakte dig igen – men selvfølgelig kun, hvis du selv har lyst til det.

Husk, vi behandler din henvendelse helt fortroligt.

SletDet har samlet en del vejledninger (<https://redbarnet.dk/sletdet/slettevejledninger/>) i, hvordan man kan slette og anmelde informationer, billeder og videoer til forskellige sociale medier, og hvordan man kan slette sine profiler. Der findes vejledninger for Ask.fm, Facebook, Instagram, Musical.ly, Skype, Snapchat og YouTube.

Under Gode råd (<https://redbarnet.dk/sletdet/gode-raad/>) findes en liste med gode råd til, hvad man kan gøre, hvis man har fået delt nogle af sine private informationer, billeder eller videoer og føler sig krænket:

- **Undersøg, hvor mange der har haft adgang til dine informationer eller set dit billede eller din video.** Har det kun ligget på din kammerats telefon, i en privat Facebookgruppe, eller har det ligget helt offentligt på Instagram eller en blog? Søg på dit navn på Google og andre søgemaskiner for at finde ud af, hvad der ligger af information om dig på nettet.
- **Bed personen slette det omgående.** Hvis det er en, som du kender, så bed personen gøre det, mens du ser på det. Så kan du føle dig helt sikker på, at det er slettet. Hvis det er på en hjemmeside, så anmeld det til ejerne af hjemmesiden.
- **Tag billeder eller screenshots** af de krænkende billeder, videoer eller tekster, hvis ikke personen vil slette indholdet omgående. Så har du beviser for, hvad der er sket. Spørg gerne en voksen, du stoler på, eller en ven/veninde om hjælp til at indsamle beviserne.
- **Kontakt det sociale medie.** Delte informationer, billeder og videoer kan desværre hurtigt forlade en enkelt Facebookprofil, hvis en person deler det videre med sine andre venner. Her på SletDet har vi slettevejledninger til, hvordan du kontakter de sociale medier og beder om at få noget slettet. Vær opmærksom på, at du skal give gode grunde til de sociale medier for at få noget slettet. Det kan for eksempel være, at det krænker dit privatliv, fordi en anden har oprettet en falsk profil med dit navn og billede, eller at det er imod det sociale medies egne regler om nøgenbilleder. Det kan tage lang tid, før de sociale medier svarer dig, og nogle gange kræver det, at man skriver flere gange.
- **Fortæl det til en voksen, som du stoler på.** Mange voksne forstår mere, end man tror, og de kan være med til at understrege alvoren over for den person, som har delt

informationer, billeder eller videoer uden dit samtykke. Det kan for eksempel være en forælder, lærer eller skolens SSP-medarbejder. Du kan også kontakte os her på Slet-Det.

8 Udenlandske lektioner

Som beskrevet i kapitel 5 savner identitetsmisbrugsudsatte støtte og opbakning fra det danske (rets)samfund. Selvom der de sidste år er kommet en del tiltag til at hjælpe identitetsmisbrugsudsatte i Danmark – som beskrevet i kapitel 7 – kan det være gavnligt at se, hvilke tiltag der findes i andre lande. I kapitel 2 er der redegjort for de anvendte undersøgelsesmetoder, og her er det beskrevet, at vi har set nærmere på identitetsmisbrug i Norge, Holland og Storbritannien. I den forbindelse har vi forsøgt at danne os et billede af definitionen på og omfanget af identitetsmisbrug i disse lande sammenlignet med Danmark. Desuden har vi undersøgt, om der findes lovende, ikke i Danmark eksisterende initiativer til at hjælpe identitetsmisbrugsudsatte.

Gennemlæsning af relevant litteratur, hjemmesider og medieindslag samt interviewsamtaler med nøglerespondenter peger på to punkter, hvor Danmark adskiller sig fra disse lande. Det er for det første en særskilt paragraf i straffeloven omhandlende identitetsmisbrug og for det andet et nationalt støttecenter for identitetsmisbrugsudsatte. Vi vender tilbage til disse to emner i henholdsvis afsnit 8.2 og 8.3. Dette kapitel starter dog med en gennemgang af afgrænsningen og omfanget af identitetsmisbrug i Norge, Holland og Storbritannien i forhold til Danmark (afsnit 8.1).

8.1 Definition på og omfang af identitetsmisbrug i de undersøgte lande

Som sagt har vi forsøgt at danne os et billede af, hvordan identitetsmisbrug defineres i Norge, Holland og Storbritannien, og af, om der findes statistik for omfanget af dette fænomen.

8.1.1 Norge

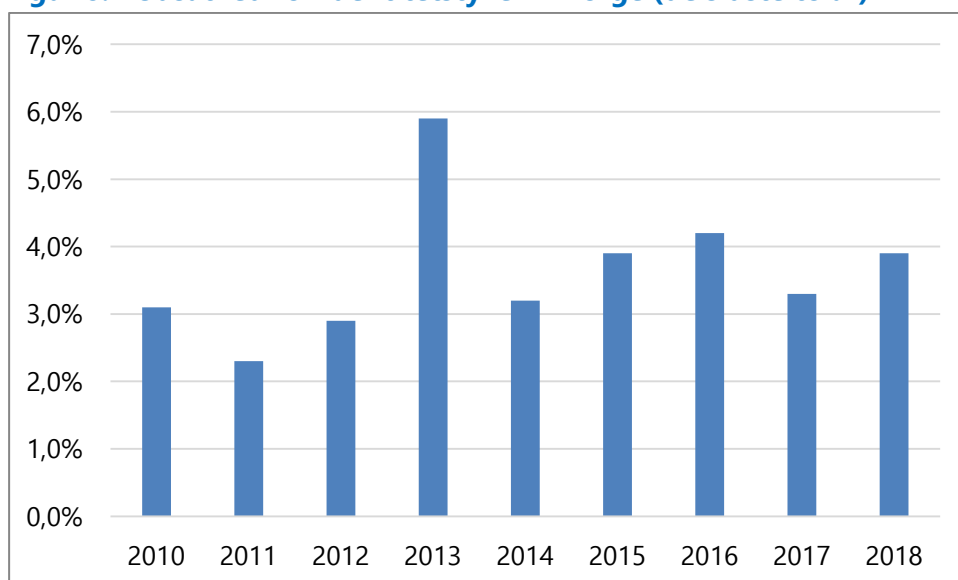
På Nettvett.no⁴⁵ påpeges det, at identitetstyveri finder sted, når nogen anskaffer, overfører, besidder eller fremstår som rette indehaver af personlige oplysninger tilhørende en privatperson eller et selskab på en uautoriseret måde, i den hensigt at begå bedrageri eller anden kriminalitet. Personlige oplysninger kan f.eks. være fødselsnummer, brugernavne, passwords/pinkoder, sundhedsoplysninger eller andre følsomme persondata. Vi må antage, at

⁴⁵ På Nettvett.no findes oplysninger, råd og vejledning om internetsikkerhed. I 2015 indgik Nasjonal Kommunikasjonsmyndighet og Nasjonal Sikkerhetsmyndighet (NSM) en samarbejdsaftale med Norsk Senter for Informasjonssikring (NorSIS) om drift af Nettvett.no.

misbrug af betalingskortoplysninger også betragtes som personlige oplysninger, for på spørgsmålet "Hvordan stopper jeg fortsat misbrug af mine personlige oplysninger?" lyder svaret bl.a.: "Du skal anmelde forholdet til politiet og kontakte alle dine aftaleparter, f.eks. kreditorer, banker og *kreditkortleverandører*" (min kursivering).

I samarbejde med Skatteforvaltningen gennemfører NorSIS en årlig undersøgelse af omfanget af ID-tyveri og identitetssikkerhed. En repræsentativ stikprøve blandt Norges befolkning over 18 år er inkluderet i undersøgelsen. Der er stillet følgende spørgsmål: "Har du i de sidste 2 år været udsat for, at en anden bruger din identitet til at begå sådanne kriminelle handlinger?" Figur 8.1 viser resultatet. Målingen fra 2013 – som dækker 2012-2013 – er markant højere end de andre målinger. Vi har ikke fundet en forklaring herpå. Ellers viser Figur 8.1, at offerrisikoen er rimeligt stabil de sidste år og svinger mellem 3 og 4 %.

Figur 8.1 Udsathed for identitetstyveri i Norge (de sidste to år)



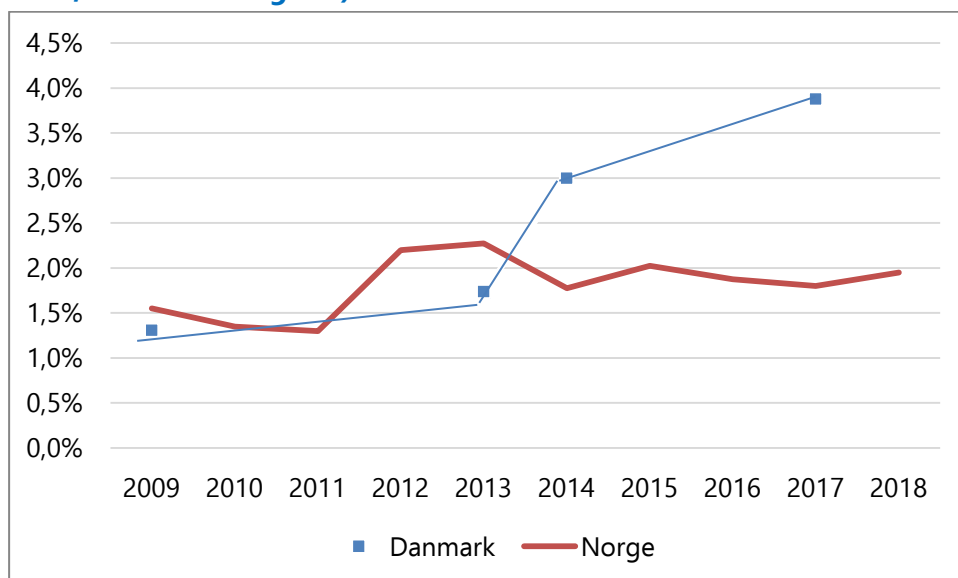
Kilde: <https://nettvett.no/sporsmal-svar-id-tyveri/>

I Danmark er der udført offerundersøgelser af bl.a. identitetsmisbrug i 2009, 2013, 2014 og 2017. Her er der blevet spurgt om, hvorvidt respondenter har været udsat for identitetsmisbrug i løbet af de sidste 12 måneder. For at kunne sammenligne de danske og norske tal er de norske tal omregnet til et estimat for udsathed på årsbasis.⁴⁶ Figur 8.2 viser resultatet. Da

⁴⁶ Det antages, at 'måling 2010' omfatter årene 2009 og 2010 og 'måling 2011' årene 2010 og 2011. Estimatet for år 2010 er beregnet som følgende: (måling 2010 + måling 2011) / 4. Denne beregningsmetode er ikke problemfri, for offerundersøgelser dør med fænomenet 'telescoping', som betyder, at respondenter har en tendens at inddrage begivenheder, der tidsmæssigt ligger uden for perioden, der spørges om. Derfor er det sandsynligt, at offerprocenten – hvis der var blevet spurgt om udsathed i de sidste 12 måneder – ville have været højere end procenttallet for to år divideret med to.

udviklingen i Norge har ligget på et stabilt niveau de sidste par år, tyder målingen fra 2017 på en stigende tendens i Danmark og ligger på et højere niveau end i Norge.

Figur 8.2 Udsathed for identitetsmisbrug (inkl. kortmisbrug) i Danmark og Norge (årsbasis; offerundersøgelse)



Kilde: Kruize 2018 (Danmark); <https://nettrett.no/sporsmal-svar-id-tyveri/> (Norge)

8.1.2 Holland

Identitetstyveri eller identitetsmisbrug er ikke begreber, som anvendes i Holland. Her bruger man begrebet *identiteitsfraude* (identitetsbedrageri). Dette begreb er bredere end identitetstyveri i Danmark. For det første henviser begrebet identitetsbedrageri ikke kun til *stjålne* identiteter, men også til *falske* identiteter. Det kan f.eks. dreje sig om asylansøgere, der benytter sig af falske identitetsbeviser. For det andet regnes misbrug med stjålne betalingskort også for en form for identitetsbedrageri.

Siden 2013 rapporterer Indenrigsministeriet en Identitetsmonitor, og fra 2014 indeholder denne monitor også oplysninger om risikoen for identitetsbedrageri. Det bemærkes, at dette begreb spænder bredt. Der er en del borgere, hvis identitet er blevet misbrugt, der mener, at begrebet 'bedrageri' er et for tungt udtryk. Under denne kategori henhører eksempelvis situationer, hvori en bekendt (ven, familie) har brugt ens navn uden samtykke, men hvor der ikke er ubehagelige konsekvenser. Dertil kommer situationer, som opfattes som irriterende. De udsatte ved ikke, hvem der står bag. Det kan dreje sig om e-mails, der bliver sendt til venner i ens navn og indeholder en opfordring til at overføre penge, fordi man er strandet et eller andet sted. Og så er der den sidste kategori af identitetsbedrageri, hvor der er tale om mere alvorlige konsekvenser, f.eks. et økonomisk tab.

I Holland er et repræsentativt udsnit af befolkningen blevet spurgt om, hvorvidt de i løbet af de sidste to år har været udsat for identitetsbedrageri – bemærk, at også i Holland, ligesom i Norge, bliver der spurgt om en periode på 2 år; i Danmark spørges der derimod kun om sidste år. Resultaterne for 2014, 2015 og 2017 var hhv. 2,1 %, 3,4 % og 5,7 %. Disse resultater indikerer, at udviklingen i Holland, ligesom i Danmark, peger på en stigende tendens. I betragtning af at de hollandske tal dækker over en periode på to år, ser det ud til, at niveauet for identitetsmisbrug i Danmark er sammenligneligt med niveauet i Holland på basis af den sidste måling (2017).

8.1.3. Storbritannien

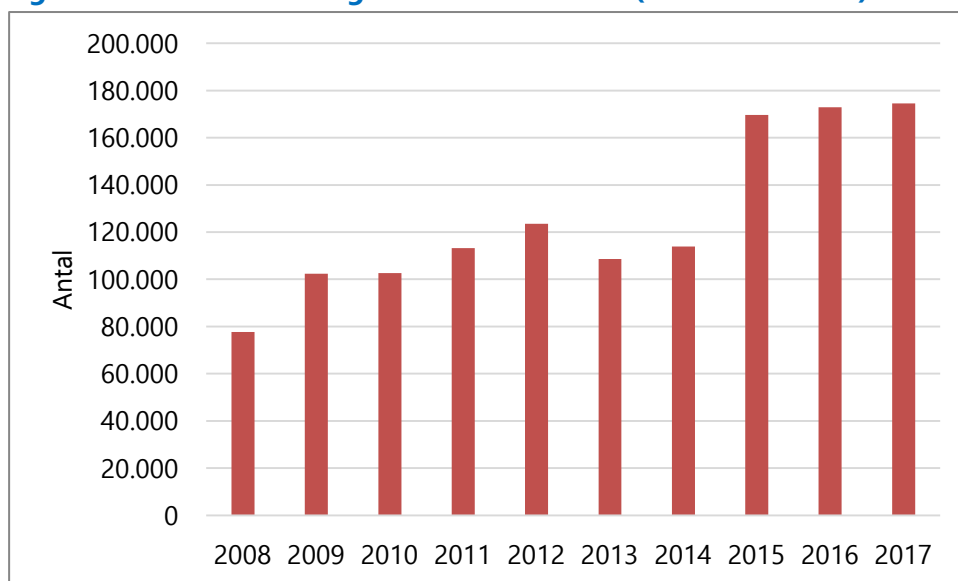
Action Fraud er Storbritanniens nationale center for bedrageri og cyberkriminalitet. Borgere og virksomheder, der har været udsat for internetrelateret bedrageri, kan anmelde sagen til Action Fraud. De skelner mellem begreberne identitetstyveri (identity theft) og identitetsbedrageri (identity fraud). Tyveri henviser til, at personoplysninger er blevet stjålet, mens bedrageri henviser til, at stjalne personoplysninger er blevet anvendt til at begå bedrageri.

Action Fraud og The Office for National Statistics publicerer ikke en statistik for hverken identitetstyveri eller identitetsbedrageri. Disse indgår i en statistik for bedrageri og computermisbrug. Cifas⁴⁷ publicerer derimod hvert år tal for identitetsbedrageri baseret på sin Fraud Database. Det er mellemorganisationer, der anmelder disse bedragerisager til Cefas. Figur 8.3 viser udviklingen siden 2008. Der har været en stigende tendens fra 2008 til og med 2012. I 2013 og 2014 faldt antallet af anmeldelser lidt for så at stige med næsten 50 % i 2015 i forhold til 2014. I 2016 og 2017 forblev niveauet mere eller mindre på 2015-niveauet.

Tal fra tre lande – Danmark, Holland og Storbritannien – viser, at der er tale om en stigende tendens i omfanget af identitetsmisbrug/bedrageri. Især de sidste par år er omfanget taget til. Norge adskiller sig fra disse tre lande; i dette land er der ikke registreret en markant stigning i omfanget af identitetstyveri de sidste par år.

⁴⁷ "Cifas is a not-for-profit fraud prevention membership organization. We are the UK's leading fraud prevention service, managing the largest database of instances of fraudulent conduct in the country. Our members are organizations from all sectors, sharing their data across those sectors to reduce instances of fraud and financial crime." (www.cifas.org.uk/about-cifas/what-is-cifas).

Figur 8.3 Identitetsbedrageri i Storbritannien (Fraud Database)



Kilde: Cifas

8.2 Identitetsmisbrug som særskilt paragraf i straffeloven

Ifølge OECD havde kun få lande en specifik lovgivning vedrørende identitetstyveri i 2009. USA må betragtes som foregangsland på dette område, idet identitetstyveri her er en selvstændig forbrydelse. I USA defineres identitetstyveri (ID Theft) på følgende vis:

Knowingly transfers, possesses, uses, without lawful authority, a means of identification of another person with the intent to commit, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law (OECD, 2009, p. 47).

Ifølge OECD (2009) betragtes identitetsmisbrug ikke som en selvstændig forbrydelse i EU-medlemsstaterne. De seneste år har flere lande dog indskrevet identitetstyveri/-misbrug/-krænkelser i deres straffelove. Selvom en sådan paragraf ikke eksisterer herhjemme, har vi haft en debat om netop dette. Det ser vi nærmere på i afsnit 8.2.1. Norge har i 2009 som det første skandinaviske land indført en særskilt paragraf i straffeloven om identitetskrænkelser.⁴⁸ Lovparagraffens ordlyd og de norske lovgiveres overvejelser i forbindelse med indførelsen af

⁴⁸ I Sverige blev identitetsmisbrug skrevet ind i straffeloven d. 1. juli 2016. Ifølge paragraf 6b i straffelovens kapitel 4 kan ulovlig brug af en anden persons identitetsdata med skade eller ulempe som følge (uautoriseret identitetsbrug) straffes med bøde eller fængsel i højst to år.

Den som genom att olovligen använda en annan persons identitetsuppgifter utger sig för att vara honom eller henne och därigenom ger upphov till skada eller olägenhet för honom eller henne, döms för olovlig identitetsanvändning till böter eller fängelse i högst två år (Brottsbalk 4. kap., § 6B, Sverige)

denne bestemmelse beskrives i afsnit 8.2.2. Straffelovsparagraffen om identitetsmisbrug blev i 2016 introduceret i Holland. I afsnit 8.2.3 beskrives paragraffens ordlyd og de hollandske lovgiveres overvejelser ved indførelsen af denne bestemmelse. I Storbritannien er identitetsmisbrug ikke en særskilt paragraf i straffeloven og har efter vores vidende heller ikke været genstand for debat.

8.2.1 Danmark

Identitetstyveri er et ofte anvendt begreb, som dog i Danmark ikke har en juridisk definition. Adspurgt har rigsadvokaten svaret retsudvalget, at en falsk profil på internettet, hvor nogle udgiver sig for at være en anden eksisterende person, som udgangspunkt ikke i sig selv kan betragtes som strafbar. Rigsadvokaten tilføjer, at der imidlertid kan være tale om strafbare forhold i forbindelse med en sådan handling (Justitsministeriet, 2009, s. 2):

Efter omstændighederne vil oprettelsen af en falsk internetprofil, hvorved man udgiver sig for at være en anden eksisterende person – og i den forbindelse videregiver oplysninger om den pågældende – imidlertid kunne udgøre en overtrædelse af straffelovens § 264 d. Efter denne bestemmelse straffes den, der uberettiget videregiver meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden. Det er uden betydning for strafbarheden, om meddelelsen er sand.

Tilsvarende må det antages, at oprettelsen af en profil på internettet i en andens navn efter omstændighederne vil kunne udgøre en overtrædelse af straffelovens § 267, hvorefter den, som krænker en andens ære ved fornærmelige ord eller handlinger eller ved at fremsætte eller udbrede sigtelser for et forhold, der er egnet til at nedsætte den fornærmede i medborgeres agtelse, straffes.

I Danmark har der været debat om, hvorvidt identitetstyveri skal være et selvstændigt begreb i straffeloven. Dansk Folkeparti fremsatte den 26. oktober 2011 et forslag til folketingsbeslutning om en særskilt straf for identitetstyveri og identitetssvindel (2011/1 BF 3). Forslaget førstebestemmedes i Folketinget den 17. januar 2012 og blev henvist til behandling i retsudvalget, som afholdt en høring den 8. maj 2012. Det viste sig, at der ikke var politisk flertal for en særskilt straffebestemmelse for identitetstyveri. Et mindretal i retsudvalget opfordrede efterfølgende regeringen til at iværksætte initiativer, der sikrer, at myndigheder, virksomheder og privatpersoner står bedst muligt rustet over for identitetstyveri og de kriminelle følger heraf. Desuden opfordrede mindretallet regeringen til i den kommende tid tæt at følge de norske erfaringer og den norske praksis i forhold til en særskilt straffelovsparagraf vedrørende identitetssvindel. Herudfra kan det løbende overvejes, om en indførelse af en sådan særskilt straffelovsparagraf vil tjene et formål i dansk sammenhæng.

Dansk Folkeparti har igen fremsat et lovforslag om en særskilt straf for identitetstyveri og identitetsmisbrug d. 14. april 2016 (B 186). I bemærkningerne til forslaget nævnes bl.a., at der er indført adskillige tiltag i forbindelse med identitetstyveri/-misbrug siden 2011/2012. I 2014 er det blevet muligt at anmode om et nyt cpr-nummer i forbindelse med identitetsmisbrug. Folketinget vedtog den 25. marts 2014 en ændring af cpr-loven (se også afsnit 7.2). Dansk Folkepartis lovforslag B 186 er dog aldrig blevet behandlet i Folketinget og er bortfaldet. Et lovforslag bortfalder automatisk, hvis ikke det er vedtaget ved folketingsårets afslutning (første tirsdag i oktober).

I anledning af lovforslaget om en særskilt kriminalisering af identitetstyveri i 2012 begrundede Justitsministeriet sin afvisning med to argumenter. For det første påpegedes det, at identitetstyveri allerede er kriminaliseret i en række straffelovsbestemmelser. For det andet vil en særskilt lovparagraf være unødigt kompleks.

Når det gælder spørgsmålet om en særskilt kriminalisering af identitetstyveri, indeholder straffeloven allerede i dag en række bestemmelser – herunder reglerne om formueforbrydelser og freds- og ærekrænkelser – som dækker denne form for kriminalitet. De handlinger, der vedrører misbrug af en andens identitet, og hvor der i praksis kan være behov for et strafferetligt værn, er således allerede kriminaliseret.

Hertil kommer, at identitetstyveri spænder meget vidt. En særskilt bestemmelse herom ville således i givet fald skulle omfatte såvel meget alvorlige former for formueforbrydelser begået ved identitetstyveri, herunder groft bedrageri med en strafferamme på helt op til 8 års fængsel, som tilfælde, der (i dag) falder helt uden for det strafferetlige område. Når henses til ønsket om størst mulig præcision og forudsigelighed i straffelovgivningen, vil det kunne være vanskeligt at indordne en egentlig strafbestemmelse om identitetstyveri i den systematik, som straffeloven bygger på. En sådan særregel vil kunne medføre afgrænsnings- og sammenstødsproblemer og dermed være unødigt kompliceret i lyset af, at identitetstyveri allerede er kriminaliseret i de situationer, hvor det kan være praktisk relevant.

(Besvarelse af 29. februar 2012 af retsudvalgets spørgsmål nr. 5 vedrørende beslutningsforslag nr. B 3, 2011-2012.)

At alle former for identitetsmisbrug er dækket af allerede eksisterende straffelovsbestemmelser nuanceres af Straffelovsrådet. Straffelovsrådet har i sin betænkning om freds- og ærekrænkelser (2017) overvejet, om der er grundlag for særskilt at kriminalisere brug af en andens identitet (identitetstyveri eller identitetsmisbrug). Rådet bemærker, at kun den mildeste form for identitetstyveri – at udgive sig for at være en anden, herunder ved oprettelse af en Facebook-profil i en andens navn – ikke allerede er strafbar. Derfor mener rådet ikke, at der er behov for yderligere kriminalisering af identitetstyveri, selvom sådanne former for identitetstyveri kan være meget generende for de personer, som får misbrugt deres identitet (Straffelovsrådet, 2017, s. 126).

8.2.2 Norge

I Norge er identitetsmisbrug efter den nye straffelov (2009) en selvstændig forbrydelse. Den nye bestemmelse om identitetskrænkelser giver straf til den, som tager en andens identitet, optræder med en andens identitet eller optræder med en identitet, som er let at forveksle med en andens. I tillæg omfattes det at sætte sig i besiddelse af en andens identitetsbevis. Identitet kan indbefatte navn, fødselsnummer, organisationsnummer, e-postadresse eller andre oplysninger, som alene eller sammen med anden information kan identificere en fysisk eller juridisk person.

Med bot eller fængsel 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.

(Straffelovens § 202, Norge)

I det norske forarbejde til bestemmelsen om identitetskrænkelser påpeges det, at mange handlinger, der omfattes af den nye bestemmelse, allerede er strafbare under den gamle straffelov. Det gælder bl.a. bedrageribestemmelser. Hvis der skal kunne være tale om en straffesag, er det dog her en forudsætning, at en stjålet identitet bruges til at udføre en strafbar handling. Den nye straffebestemmelse gør det enklere at strafforfølge identitetstyveri, idet det nu er lettere at bevise identitetskrænkelser end et forsøg på fuldbyrdet bedrageri.

Identitetskrænkelser kan krenke menneskers integritet og sikkerhed uafhængig af om den rent faktisk fører til videre lovbrud eller ikke. Det vil også være enklere at bevise identitetskrænkelser end (forsøg på) den fuldbyrdede bedragerihandlingen. (Ot. Prp. nr. 22 (2008-2009), side 44 f.)

I det svenske forarbejde til bestemmelsen om ulovlig identitetsanvendelse påpeges i øvrigt ligeledes, at der vil være overlap med andre lovbestemmelser, primært formueforbrydelser, men også dokumentfalsk og falsk vidne. Der forventes 'konkurrence'-situationer, og det bemærkes, at de generelle regler om konkurrerende bestemmelser er gældende. Formålet med lovbestemmelsen er at modvirke misbrug af identitetsdata og beskytte mod integritetskrænkelser.

Både den norske og den svenske lovgiver anerkender dermed det fremsatte argument fra den danske lovgiver, at mange former for identitetstyveri/-misbrug allerede er kriminaliseret, men de ser stadig fordele i en særskilt lovbestemmelse. I forhold til det danske Justitsministeriums bemærkning om, at identitetstyveri spænder meget vidt, som argument imod en særskilt bestemmelse, kan det bemærkes, at den norske lovgiver ikke har indført en egen be-

stemmelse for *grov* identitetskrænkelse, netop fordi handlingen ofte vil være en forberedelseshandling til anden kriminalitet, og dermed betragtes strafferammen som tilstrækkeligt høj.

Ved siden af spørgsmålet om, hvorvidt identitetstyveri/-misbrug er kriminaliseret i allerede eksisterende lovparagraffer, nævner Dansk Folkeparti to begrundelser for, at der er et behov for en selvstændig bestemmelse for identitetstyveri og identitetsmisbrug (Lovforslag B 186, 2015-2016):

- 1) Et klart signal om, at det er et kriminalitetsområde, der skal prioriteres i langt højere grad.
- 2) En selvstændig registrering, så udviklingen i denne kriminalitetsform kan følges nøje.

Om disse argumenter holder vand, kan ikke fastslås, uden at der indføres en særskilt bestemmelse for identitetstyveri/-misbrug i Danmark. De norske erfaringer kan dog give et fingerpeg om, hvordan en sådan bestemmelse fungerer i praksis. Den norske straffelovsparagraf 202 er, som sagt, indført i 2009. Under en studietur til Norge i februar 2018 har jeg bl.a. forsøgt at få svar på spørgsmålet om, hvorvidt identitetstyveri/-misbrug er prioriteret i højere grad efter indførelsen af denne paragraf i straffeloven. Det er klart, at et grundigt svar kræver mere end et par interviewsamtaler med repræsentanter for aktører på dette område, men disse samtaler peger i retning af, at indførelsen af lovparagraffen ikke har ført til de store forandringer i politiets efterforskningsarbejde.

Gevinsten ligger ved anmeldelsesprocessen. Udsatte for identitetstyveri/-misbrug kan anmelde sagen uden risiko for at blive afvist af politiet. Det vil ikke sige, at det fører til en pålidelig statistik. Af Politidirektoratet fik jeg en oversigt over 'ID-sager' for 2016 (615 sager) og 2017 (547 sager), som skulle omfatte § 202-sager. Oversigten viste også, at ca. halvdelen af disse sager var henlagt af politiet. Politiets repræsentant forklarede, at mange sager om identitetsmisbrug ikke registreres som ID-sager, men f.eks. som bedragerisager. Han havde søgt i politiets systemer på bedrageri med ID som modus, og det gav som resultat 1.185 sager i 2016 og 1.573 sager i 2017. Ca. tre ud af fire af disse sager er henlagt af politiet.

Selvom § 202 blev indført i 2009, findes der kun tilgængelig selvstændig statistik for perioden efter oktober 2015 på Statistisk Sentralbyrås hjemmeside (www.ssb.no). Der skelnes mellem to former for identitetskrænkelse: 1) befatning med annens identitetsbevis og 2) opptre med annens identitet. At handle med en anden persons identitetsbevis er blevet anmeldt 471 gange i 2016 og 466 gange i 2017. At optræde med en anden persons identitet har ført til 2.098 anmeldelser i 2016 og 2.774 anmeldelser i 2017.

Lovparagraffen om identitetskrænkelser har ført til en statistik i Norge, men om statistikken nøje viser udviklingen for identitetstyveri/-misbrug, er tvivlsomt. Dermed dæmper erfaringerne fra Norge forventningerne til en særskilt bestemmelse i Danmark i forhold til opprioritering af og overblik over denne kriminalitetsform.

8.2.3 Holland

I Holland er identitetsmisbrug kriminaliseret i straffelovens paragraf 231b, som er indført 1. maj 2014. Strafferammen går op til 5 års fængsel. Det fremgår af paragraf 231b, at:

- der skal være tale om forsæt
- formålet skal være enten at skjule sin egen identitet eller at misbruge en andens identitet
- der skal være forvoldt skade.

Efter fremsættelsen af lovforslaget i parlamentet blev justitsministeren bl.a. spurgt om, hvorvidt han kunne redegøre for, hvilke situationer der omfattes af paragraf 231b. Ministeren fremlagde derefter to eksempler:

- 1) En situation, hvori der lejes noget i en andens navn, og udlejer sender regningen til denne person. Altså et eksempel på økonomisk skade som følge af identitetsmisbrug.
- 2) En situation, hvori en person opretter en profil i en andens navn og efterfølgende krænker vedkommendes omdømme.

Paragraf 231bs begreb 'skade' kan så stå for økonomisk skade. Dermed får offeret mulighed for at bede anklageren/dommeren tage stilling til et erstatningskrav under den strafferetlige behandling af sagen og behøver ikke nødvendigvis at anlægge et civilretligt søgsmål. I en retssag (RBNHO:2017:3643), hvor tiltalte havde brugt anmelderens Facebook-billeder i en sex-annonce på nettet, blev tiltalte dømt, men ikke efter paragraf 231b. Retten slog fast, at paragraf 231b ikke kunne anvendes, for et billede er ikke i sig selv en personoplysning.

8.3 Nationalt støttecenter

I Danmark har Digitaliseringsstyrelsen den nationale, koordinerende rolle i forbindelse med vejledning og rådgivning ved identitetsmisbrug. De står bag den digitale vejledning og rådgivning, som er tilgængelig på borger.dk (omtalt i kapitel 7). Digitaliseringsstyrelsen står også – i samarbejde med KL, Danske Regioner, DKCERT og DelC – for den årlige undersøgelse af

danskernes informationssikkerhed.⁴⁹ Der findes imidlertid ikke i Danmark et nationalt støttecenter, som kan hjælpe identitetsmisbrugsudsatte.

I Holland oprettedes d. 1. marts 2010 et Nationalt Center for Identitetsmisbrug (på hollandsk *Centraal Meldpunt Identiteitsfraude en -fouten*; CMI) – efter en pilotperiode, der havde løbet siden november 2008. Dette center hører under Indenrigsministeriet. Vi ser nærmere på dette center i afsnit 8.3.1.

I Norge findes NorSIS – *Norsk senter for informasjonssikring* – som blev stiftet d. 2. februar 2010. NorSIS er en videreførelse af Senter for informasjonssikring (SIS), som blev etableret d. 1. april 2002 som et pilotprojekt ved Handels- og Næringsdepartementet. I januar 2006 blev SIS omdannet til NorSIS, med Gjøvik Kunnskapspark som operatør. I februar 2010 blev NorSIS reorganiseret og etableret som en ideel og uafhængig medlemsforening. NorSIS modtager årligt tilskud fra det norske Justis- og Beredskapsdepartement. NorSIS bliver nærmere belyst i afsnit 8.3.2.

I Storbritannien findes *Action Fraud*, hvor alle bedragerianmeldelser modtages og – hvis der findes efterforskningsspor – sendes videre til politidistrikterne for nærmere efterforskning. Action Fraud er ikke et nationalt støttecenter, men har også til formål at rådgive og vejlede anmeldere af identitetsmisbrug. Action Fraud ligner til forveksling det nyoprettede Landsdækkende Center for It-relateret økonomisk Kriminalitet (LCIK), og derfor omtales Action Fraud ikke nærmere i denne rapport.⁵⁰

8.3.1 CMI i Holland

I Holland ligger det overordnede ansvar for identitetsmisbrug i Indenrigsministeriet. Det Nationale Center for Identitetsmisbrug (CMI) hører under Indenrigsministeriet og er oprettet i november 2008 som en pilotordning. CMI startede som fast ordning den 1. marts 2010. Centret har to kerneopgaver. For det første tilbydes CMI-rådgivning, vejledning og praktisk assistance til identitetsmisbrugsudsatte på basis af personlig kontakt. Den praktiske assistance er problemorienteret. CMI påtager sig en koordinerende rolle og kontakter, om nødvendigt, andre aktører på vegne af offeret. Det kan ske i samarbejde med politiet og anklagemyndigheden, men også andre myndigheder.

⁴⁹ Den seneste udgave af denne undersøgelse er fra december 2018 og kan hentes her:

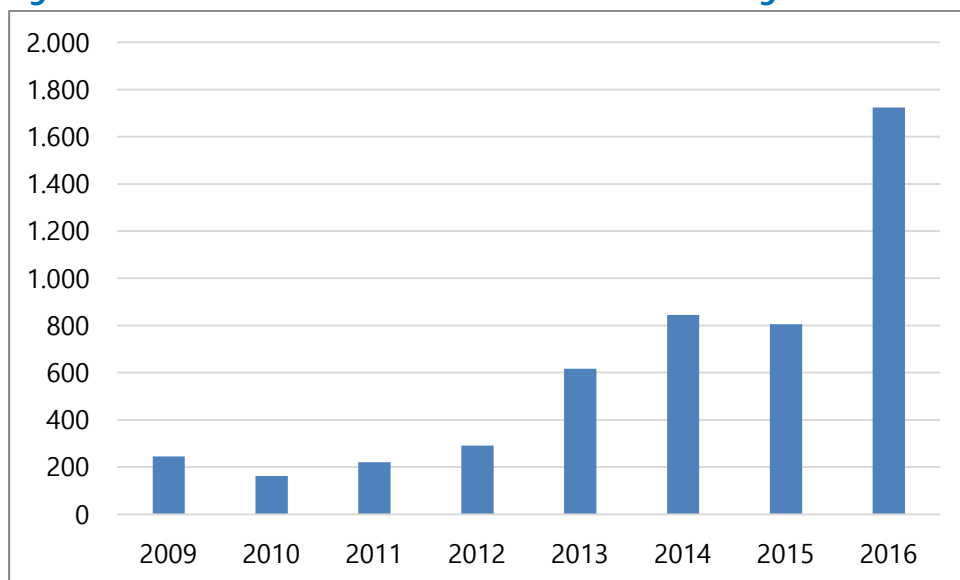
https://digst.dk/media/18755/danskernes_informationssikkerhed_december_2018_191218.pdf

⁵⁰ Et par uger før jeg havde en aftale ved Action Fraud, havde en delegation fra Københavns Politi været på besøg, og Action Fraud har klart været en inspirationskilde til oprettelsen og indretningen af LCIK.

CMI's anden kerneopgave er at opbygge viden om fænomenet identitetsmisbrug. Det sker på den ene side ved registrering af udsattes henvendelser og deres sagsforløb. På den anden side indhentes oplysninger hos relevante partnere og ved indsamling af (trend)rapporter. På baggrund af denne viden udarbejdes der kampagnemateriale og skrives notater til (politiske) beslutningstagere. CMI's medarbejdere optræder i pressen, bidrager til debatter og deltager i konferencer.

Figur 8.4 viser, at antallet af henvendelser til CMI tager til med årene. Ifølge respondenterne fra CMI – som blev interviewet i forbindelse med et forskningsophold i Holland – betyder denne stigning ikke nødvendigvis, at der er flere tilfælde af identitetsmisbrug. Det kan også (til dels) skyldes en tiltagende anmeldelsestilbøjelighed på grund af en større bevidsthed i befolkningen om identitetsmisbrug og et stigende kendskab til CMI som følge af kampagner.

Figur 8.4 Antallet af henvendelser om identitetsmisbrug til CMI



Kilde: CMI

8.3.2 NorSIS i Norge

NorSIS er en uafhængig medlemsforening, der modtager tilskud fra Justis- og Beredskapsdepartementet for ca. halvdelen af de samlede udgifter. Informationssikkerhed er NorSIS' kerneforretning, og de retter sig primært mod små og mellemstore virksomheder. Men NorSIS lægger også vægt på rådgivning og vejledning af borgere.

Erfaring viser at den generelle befolkningsinformasjonen i stor grad også videreføres til de små og mellomstore virksomhetene gjennom deres ansatte. Informasjon til befolkningen er også viktig for å skape sikkerhetskompetansen som kreves som en del av regjeringens digitalisering av Norge (Halvårsrapport NorSIS 2018, s. 11).

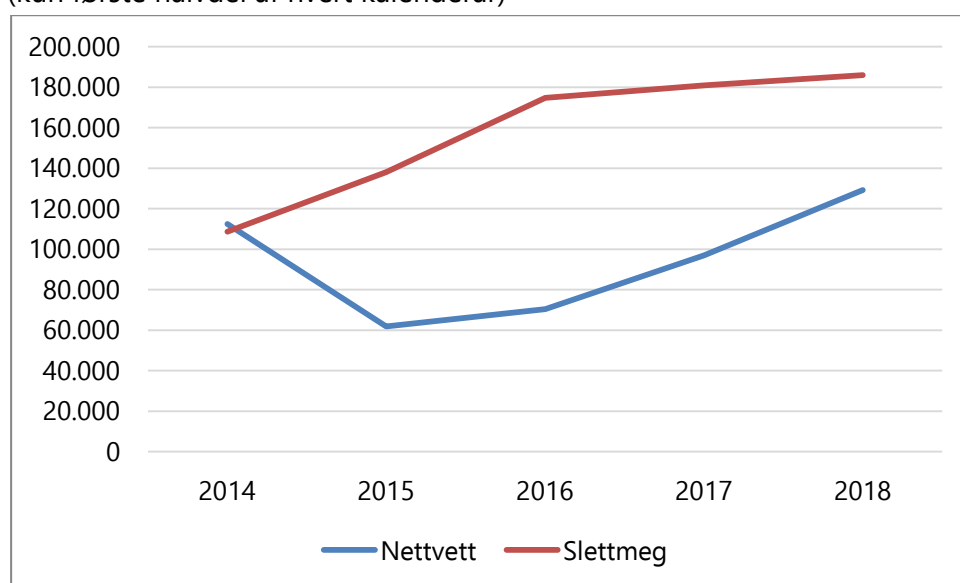
I forhold til borgerne har NorSIS to vigtige produkter. For det første har de samlet en oversigt over vejledninger om informationssikkerhed. Disse vejledninger er tilgængelige på hjemmesiden www.nettvett.no/veiledninger/. Der ligger vejledninger vedrørende identitetstyveri og bedrageri på nettet, men også om internetbrug og sociale medier. Nettvett.no blev etableret i starten af 2017. Før 2017 var disse vejledninger tilgængelige på norsis.no.

Det andet produkt er Slettmeg (www.slettmeg.no). Her kan man downloade vejledninger i, hvordan man sletter (falske) profiler fra Facebook, Snapchat, Instagram, Twitter osv., og i, hvordan man sletter et hit i søgemaskiner og netkataloger. Slettmeg kan også kontaktes personligt – enten ved at udfylde et skema (skriftlig henvendelse) eller ved at ringe til en rådgiver. Årligt henvender 5-6.000 personer sig personligt til Slettmeg.

Figur 8.5 viser antallet af unikke besøgende på Norsis/Nettvetts og Slettmegs hjemmesider i perioden 2014-2018. Det er antallet af besøgende i det første halvår af et kalenderår. På årsbasis er antallet af besøgende – må vi antage – dobbelt så stort.

Figur 8.5 Antallet af unikke besøgende på Nettvetts og Slettmegs hjemmesider

(kun første halvdel af hvert kalenderår)



Kilde: Halvårsrapport NorSIS 2018, s. 21

9 Konklusioner og overvejelser

I dette sidste kapitel drages konklusioner med afsæt i problemstillingerne, formuleret i afsnit 1.2. Rapporten slutter af med enkelte overvejelser over, hvordan identitetsmisbrugsudsatte kan hjælpes bedre, når skaden er sket.

9.1 Identitetsoplysninger

På den ene side er der spørgsmålet om, hvilke identitetsoplysninger der danner grundlag for misbrug, på den anden side spørgsmålet om, til hvilket formål disse oplysninger bliver misbrugt. Der skelnes mellem økonomisk misbrug og ærekrænkende misbrug. Der findes identitetsoplysninger, som typisk bliver anvendt ved økonomisk misbrug, og oplysninger, som bliver brugt til et krænkende formål, men opdelingen er ikke knivskarp.

Betalingskortoplysninger bruges helt overvejende mest ved økonomisk misbrug. I Danmark regnes betalingskortmisbrug ikke for identitetsmisbrug. Det kan diskuteres, men faktum er, at skaden ved kortmisbrug ofte er begrænset, og at det er sjældent, at borgeren hæfter for tabet; det sker kun, hvis vedkommende har opført sig groft uagtsomt. Misbrug af danske betalingskort foregår for en stor dels vedkommende på udenlandske e-handelsmarkeder.

Når det kommer til de mere belastende former for økonomisk identitetsmisbrug, er det typisk to typer identitetsoplysninger, der bliver misbrugt: et kørekort/pas eller NemID. Kørekortet og/eller passet kan være tabt eller stjålet. Med et sådant dokument kan der f.eks. købes på kredit, og det foregår typisk i fysiske butikker. Når der bliver oprettet et lån eller købt på kredit på nettet, kræves der typisk NemID-validering.

Misbrug af sociale mediers profiler, billeder og e-mailkonti kan ske med et økonomisk sigte, f.eks. ved romance scam, men kan også have til formål at krænke en anden person. Det er ikke altid klart, hvorfor disse personoplysninger bliver misbrugt.

9.2 Instanser og dokumentationskrav

Når en person er blevet udsat for økonomisk identitetsmisbrug, er det vigtigt, at han eller hun reagerer hurtigt. Typisk skal man kontakte den instans, der har udstedt det misbrugte dokument – kommunen ved misbrug af pas, kørekort eller sundhedskort; banken eller kortselskabet ved misbrug af betalingskort. Hvis der er trukket et beløb fra udsattes konto, skal

der gøres indsigelse. Det samme gælder, hvis et firma kræver betaling for en vare eller ydelse, som er bestilt af gerningsmanden. Det kræves en politianmeldelse af episoden, hvis der gøres indsigelse. Det er et krav fra den instans, der skal føre beløbet tilbage eller slette regningen.

Det er forskelligt fra virksomhed til virksomhed, hvor villige de er til at slette regningen, hvis en person påstår, at han/hun har været udsat for identitetsmisbrug. Det afhænger af, hvilke oplysninger der er blevet misbrugt. Hvis det handler om virksomheder, der tilbyder et forbrugslån, og låneaftalen er underskrevet med NemID, er der stor sandsynlighed for, at virksomheden holder fast i sit krav. Der er ligeledes stor sandsynlighed for, at den får medhold i fogedretten, hvis det kommer til et retsligt opgør. Det skyldes, at den påstået udsatte enten har været vidende om, at hans/hendes NemID-oplysninger blev misbrugt, eller at vedkommende har handlet groft uagtsomt med sine oplysninger. Socialt udsatte og svage borgere er forholdsvis ofte dem, der er udsat for (mis)brug af deres NemID-oplysninger.

Når det handler om krænkende misbrug, så er det langt fra sikkert, at politiet vil optage en anmeldelse. Det afhænger af, hvad der er sket, og hvilke oplysninger der er blevet misbrugt. Hvis oplysninger er blevet stjålet ved hjælp af hacking, optager politiet anmeldelsen. Det samme gælder deling af nøgenbilleder af mindreårige (børnepornografi). Men hvis en persons (profil)billeder er blevet misbrugt til at oprette en falsk profil, betragter politiet episoden som et privat anliggende. Den udsatte kan gå den civilretlige vej, men det kræver, at gerningsmanden er kendt – og det kan være svært, når politiet ikke vil efterforske sagen.

Når en person vil fjerne en falsk profil i sit navn eller krænkende indhold fra nettet, så kræver det, at der bliver taget kontakt til den pågældende internettjeneste. Den kræver beviser fra den udsatte for, at det er ham eller hende, der er den rette person. Det er i sig selv logisk nok, men det betyder, at man skal uploade en kopi af et identitetsbevis, efter at man har været udsat for misbrug af personoplysninger.

9.3 Psykiske konsekvenser

Hvis økonomisk identitetsmisbrug har psykiske konsekvenser for offeret, bunder det ofte i frygt for konsekvenserne og/eller fremtiden. Det kan være i en mild grad – frygt for, at der kommer flere regninger, og tvivl om, hvorvidt man hæfter for (en del af) tabet – men det kan også udvikle sig til decideret angst for fremtiden. Identitetsmisbrug rækker ved den udsattes fundament i livet. De psykiske konsekvenser minimeres, hvis den udsatte føler sig støttet af myndighedsinstanser og samfundet, og hvis politiet optager anmeldelserne og støtter de udsatte i deres følelse af, at der er gjort dem uret – i stedet for at de får at vide, at de ikke er den forurettede part i lovens forstand, eller at politiet ikke kan bruge kræfter på sådan noget.

Det samme gælder for andre instanser som kommuner, kreditorer, banker osv.; om de giver støtte eller modspil.

Ved krænkende identitetsmisbrug spiller frygt også en vigtig rolle. Frygt for, hvem der står bag chikanen, hvordan omverdenen vil reagere, om det er muligt at få slettet materiale osv. Også her spænder de psykiske konsekvenser fra ubehag til decideret angst eller depression. Identitetsmisbrug kan føre til, at offeret melder sig syg fra sit arbejde. En del udsatte opsøger en psykolog. Der findes dog ikke tal på, hvor stor en del af ofrene der lider af store psykiske konsekvenser af misbruget af deres identitetsoplysninger.

9.4 Økonomiske konsekvenser

Krænkende identitetsmisbrug har ikke direkte økonomiske konsekvenser for offeret, men der kan sagtens være indirekte omkostninger i form af tid, der skal bruges til oprydningsarbejde, tabt arbejdsfortjeneste eller udgifter til advokatbistand. Der er dog instanser, der hjælper gratis med at slette ulovligt indhold fra nettet – Red Barnet (mindreårige) og Dansk Kvinde-samfund (voksne). Hvis den pågældende har en familieforsikring, der dækker Web Cleanup, kan der også trækkes på hjælp fra denne side.

Ved økonomisk misbrug er der ikke kun indirekte økonomiske konsekvenser, men også direkte omkostninger. Offerundersøgelsen Internetkriminalitet 2017 indikerede, at virksomhederne står for ca. 90 % af tabet, mens udsatte, hvis identitet er blevet misbrugt, hæfter for ca. 10 % af tabet. Især når NemID-oplysninger er blevet (mis)brugt, er der stor sandsynlighed for, at offeret/det påståede offer hæfter for tabet. Det er dog tvivlsomt, hvorvidt den pågældende er i stand til at betale regningen. Denne tvivl gælder i hvert fald for socialt udsatte, som typisk modtager bistand.

9.5 Eksisterende tiltag

Der eksisterer en stribe tiltag til at hjælpe identitetsmisbrugsudsatte. Når det handler om økonomisk misbrug, kan offeret på borger.dk og hjemmesider fra adskillige instanser læse, hvordan man skal forholde sig. Også app'en Mit Digitale Forsvar indeholder en 'førstehjælpskasse' med råd og vejledning om, hvad offeret bør gøre, når skaden er sket. Hvis offeret har en familieforsikring, er der stor chance for, at den pågældende kan få hjælp gennem forsikringsselskabet (ved oprydningsarbejde af Affinion). Socialt udsatte kan få støtte fra Den Sociale Retshjælps Fond.

For at undgå, at gerningsmanden bliver ved med at købe på kredit med udsattes personoplysninger, har der fra januar 2017 kunnet indsættes en kreditadvarsel i CPR. Ved udgangen af

2018 havde 35.769 danskere en aktiv advarsel på deres cpr-nummer. Siden 2014 har det også været muligt at få et nyt cpr-nummer i forbindelse med identitetsmisbrug. Denne ordning benyttes dog sjældent. I en periode på 4 år har 76 personer ansøgt om et nyt cpr-nummer på grund af identitetsmisbrug; 7 personer har fået tildelt et nyt cpr-nummer (8 ansøgninger er endnu ikke afgjort).

Når det kommer til krænkende misbrug, kan offeret også finde vejledning og gode råd på adskillige instansers hjemmesider. Red Barnet (mindreårige) og Dansk Kvindesamfund (voksne) har samlet relevante vejledninger i, hvordan man kan få slettet profiler, billeder mm. fra sociale medier og andre platforme. Udover disse vejledninger kan man komme i kontakt med en rådgiver fra disse instanser; skriftligt (pr. e-mail) eller telefonisk. Hvis offeret har en familie-forsikring, er der stor chance for, at den pågældende kan få hjælp gennem forsikringsselskabet (ved sletningsarbejde af Affinion).

9.6 Udenlandske ordninger

Der er blevet set nærmere på identitetsmisbrug i Norge, Holland og Storbritannien. I disse lande er identitetsmisbrug, ligesom i Danmark, i vækst. Undtagelsen er Norge, hvor identitetstyveri de sidste par år har set ud til at ligge på et stabilt niveau. Der findes to opsigtsvækkende tiltag i Norge og Holland i sammenligning med Danmark. For det første er identitetsmisbrug som særskilt paragraf indskrevet i straffeloven i både Norge og Holland. For det andet har disse lande et nationalt støttecenter for identitetsmisbrugsudsatte.

I Norge er identitetsmisbrug efter den nye straffelov (2009) en selvstændig forbrydelse. Den nye bestemmelse om identitetskrænkelser giver op til 2 år fængselsstraf til den, som tager en andens identitet, optræder med en andens identitet eller optræder med en identitet, som er let at forveksle med en andens. I Holland har identitetsmisbrug været kriminaliseret siden 2014. Strafferammen går op til 5 års fængsel. Der skal være tale om forsæt, og formålet skal være enten at skjule sin egen identitet eller at misbruge en anden persons identitet, og der skal være forvoldt skade.

Det hollandske Nationale Center for Identitetsmisbrug (CMI) hører under Indenrigsministeriet og oprettedes i november 2008 som pilotordning og siden marts 2010 som fast ordning. Centret har to kerneopgaver. For det første tilbydes CMI-rådgivning, vejledning og praktisk assistance til identitetsmisbrugsudsatte på basis af personlig kontakt. I 2016 modtog CMI 1.724 henvendelser fra borgere. CMI's anden kerneopgave er at opbygge viden om fænomenet identitetsmisbrug. Det sker på den ene side ved registrering af udsattes henvendelser og deres sagsforløb, mens der på den anden side indhentes oplysninger hos relevante partnere og indsamles (trend)rapporter. På baggrund af denne viden udarbejdes der kampagnemate-

riale og skrives notater til (politiske) beslutningstagere. CMI's medarbejdere optræder i pressen, bidrager til debatter og deltager i konferencer.

Det norske NorSIS er en uafhængig medlemsforening med informationssikkerhed som kerneforretning. NorSIS har to produkter. For det første har de samlet en oversigt over vejledninger om informationssikkerhed. I 2018 havde de ca. 250.000 unikke besøgende på deres hjemmeside. Det andet produkt er Slettmeg. Her kan man downloade vejledninger i, hvordan man sletter (falske) profiler fra Facebook, Snapchat, Instagram, Twitter osv., og i, hvordan man sletter et hit i søgemaskiner og netkataloger. Slettmeg kan også kontaktes personligt – enten ved at udfylde et skema (skriftlig henvendelse) eller ved at ringe til en rådgiver. 5-6.000 personer henvender sig hvert år personligt til Slettmeg. I 2018 havde de ca. 370.000 unikke besøgende på deres hjemmeside.

9.7 Overvejelser

De sidste ti år er der kommet mere opmærksomhed på identitetsmisbrug og en hel del offentlige og private initiativer til at forebygge misbrug og begrænse skaden efter misbruget. Dette forskningsprojekt viser, at der stadig er plads til forbedring. Vi vil pege på tre muligheder: 1) en særskilt straffelovsparagraf, 2) spærring af identitetsbeviser og 3) et nationalt (videns)center for identitetsmisbrug.

9.7.1 Særskilt straffelovsparagraf

Ønsket om en særskilt lovparagraf for identitetstyveri/-misbrug kan have flere begrundelser. Set med juridiske briller kan det fastslås, at langt de fleste handlinger, som kan betegnes som identitetsmisbrug, allerede er omfattet af andre bestemmelser i den danske straffelov. Det gælder dog ikke dette at udgive sig for at være en anden, herunder ved oprettelse af en Facebook-profil i en andens navn. Det vil sige identitetsmisbrug, som kan betragtes som chikane. I Danmark vil sådan en handling høre hjemme under freds- og ærekrænkelser. Netop disse artikler kendetegnes ved, at de som udgangspunkt er undergivet privat påtale, jf. straffelovens § 275.

Hvis formålet med en særskilt lovparagraf er en prioritering af området og/eller et bedre overblik, er det et spørgsmål, om disse mål ikke kan nås på en anden måde. Burde straffeloven blive brugt hertil? Kriminalisering kan også føre til uønskede sideeffekter, som påpeget af det norske datatilsyn i deres høringssvar til lovforslaget.

Hovedinnvendingen er at forslaget til straffebestemmelse kan bidra til usikkerhet knyttet til bruk av pseudonymer og kallenavn som spesielt barn og unge sterkt oppfordres til å bruke ved kommunikasjon på internett. Selv om bruk av uriktig identitet kan krenke personvernet, mener

tilsynet at slik bruk er utbredt og i de fleste sammenhenger bør anses som legitim. (Ot. Prp. nr. 22 (2008-2009), side 44 f)

Der er dog også, efter vores vurdering, gode grunde til at overveje en særskilt paragraf. I Danmark betragtes udsatte for økonomisk identitetsmisbrug ikke som udsatte i lovens forstand, for det er (for det meste) ikke dem, der lider økonomisk tab; det er banker, forretninger osv. For et par år siden blev en anmeldelse fra en person, hvis identitet ofte var blevet misbrugt, afvist med den begrundelse, at personen ikke hæftede for tabet. Denne praksis har ændret sig, men ofte oprettes der stadig ikke et såkaldt skarpt journalnummer (som optræder i kriminalstatistikken), når en person anmelder, at hans/hendes identitet er blevet (forsøgt) misbrugt.

Mest problematiske er de sager, hvori en persons identitet (navn, billeder osv.) bliver misbrugt på de sociale medier og andre steder på internettet. Så længe det ikke er seksuelt krænkende, kan politiet ikke gøre ret meget; hertil mangler politiet de rette værktøjer. Spørgsmålet er dog, om politiet ikke vil drukne i denne type sager, hvis der åbnes op for at anmelde og efterforske dem, med det resultat, at størstedelen af dem vil blive henlagt. Muligvis, men erfaringerne fra Norge viser, at politiet reelt efterforsker en del af disse sager. Et andet argument for kriminalisering af disse former for identitetsmisbrug er af mere symbolsk karakter. Det er vores vurdering, at det støder mange, at det ikke er strafbart i Danmark, når der oprettes falske profiler på nettet ved hjælp af andres personoplysninger og/eller billeder. Strafbarstillingen giver det signal, at det ikke er i orden, uanset om politiet reelt efterforsker (en del af) disse sager.

9.7.2 Spærring af identitetsbeviser

Både identitetsmisbrugsudsatte og virksomheder peger på, at det ville være gavnligt, hvis danske identitetsbeviser kunne spærres, ligesom der kan spærres for et tabt eller stjålet betalingskort. En repræsentant for Dansk Erhverv udtrykker sig således:

Både forbrugere og butikker ville være bedre beskyttet, hvis det blev muligt for borgerne at melde deres kørekort, sygesikringskort eller pas stjålet, og de kunne "spærres", som man ser det med kreditkort. Butikkerne skulle så have adgang til oplysninger om de stjålne kort. Det ville kunne afskrække svindlerne, hvis de vidste, at butikkerne kunne tjekke, om identitetskortene var stjålet. En ordning, der gør det muligt at spærre personlige identitetskort, vil kræve, at der etableres en database, og at også sygesikringskort får et nummer. Det vil selvfølgelig koste lidt på den korte bane, men det vil spare både borgere og butikker for både bekymringer og tab.

9.7.3 Nationalt center

På nuværende tidspunkt er støtte og viden om identitetsmisbrug i Danmark spredt ud over adskillige instanser, som Digitaliseringsstyrelsen, CPR-kontoret, politiet, Forbrugerrådet Tænk, Red Barnet, Dansk Kvindesamfund, Den Sociale Retshjælps Fond og forsikringsselskaberne. For identitetsmisbrugsudsatte vil det være en fordel, hvis støtten samles ét sted, og man kan komme i kontakt med en rådgiver, som ikke kun hjælper med praktiske sager, men også er forstående og medfølelse. Det vil sikkert reducere de psykiske konsekvenser af identitetsmisbrug og bidrage positivt til ofrenes syn på Danmark som retssamfund. En vigtig sideeffekt af et nationalt center for identitetsmisbrug vil være, at nye beslutninger eller tiltag i forhold til dette fænomen kan træffes mere vidensbaseret.

Litteraturliste

- Binder, R. & M. Gill (2005). Identity theft and fraud: learning from the USA. Perpetuity Research and Consultancy International.
- Det Kriminalpræventive Råd (DKR) (2016). Når forbrydelser bliver digitale: En antologi om IT-kriminalitet og adfærd på internettet.
- Digitaliseringsstyrelsen og DKCERT (2015). Borgernes informationssikkerhed 2014.
- Digitaliseringsstyrelsen og DKCERT (2017). Borgernes informationssikkerhed 2016.
- DTU Transport (2014). Transportvaneundersøgelsen, Center for Transport Analytics.
- Forbrugerrådet Tænk (2016). Digital tryghed: De væsentligste digitale udfordringer for forbrugerne i Danmark. København.
- Franks, Mary A. (2015). Drafting An Effective "Revenge Porn" Law: A Guide for Legislators, p. 1-14.
- Justitsministeriet (2009). Besvarelse af spørgsmål nr. S 1907 (Strafbare forhold i relation til såkaldt identitetstyveri og identitetsmisbrug på internettet).
- Justitsministeriets Forskningskontor (2018). Omfanget og karakteren af stalking, en befolkningsundersøgelse 2017/18.
- Kruize, Peter (2009). Identitetstyveri. Københavns Universitet: Det Juridiske Fakultet.
- Kruize, Peter (2013). Kriminalitet i en digitaliseret verden. Københavns Universitet: Det Juridiske Fakultet.
- Kruize, Peter (2015). Internetkriminalitet 2014: Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace. Københavns Universitet: Det Juridiske Fakultet og Det Kriminalpræventive Råd.
- Kruize, Peter (2018). Internetkriminalitet 2017: Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace. Københavns Universitet: Det Juridiske Fakultet og Det Kriminalpræventive Råd.
- Larsen, Henrik og Torben B. Sørensen (red) (2017). DKCERT Trendrapport 2017, Lyngby, DeiC
- OECD (2009). Online Identity Theft. OECD Publishing.
- Straffelovsrådet (2017). Betænkning om freds- og ærekrænkelser, nr. 1563.
- Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Cambridge/Malden MA: Polity.

Besvarelse af spørgsmål (Justitsministeriet), lovforslag

- B 3 Forslag til folketingsbeslutning om en særskilt straf for identitetstyveri og identitetssvindel (2011). <https://www.retsinformation.dk/Forms/R0710.aspx?id=138985>
- B 186 Forslag til folketingsbeslutning om en særskilt straf for identitetstyveri og identitetsmisbrug (2016).

<http://www.ft.dk/samling/20151/beslutningsforslag/B186/index.htm>S 1907 (strafbare forhold i relation til såkaldt identitetstyveri og identitetsmisbrug på internettet), 2009.

- Retsudvalgets spørgsmål nr. 5 (beslutningsforslag nr. B 3, 2011-2012).
- Om identitetskrænkelser i Norge. Ot. Prp. nr. 22 (2008-2009),
<https://www.regjeringen.no/no/dokumenter/otprp-nr-22-2008-2009-/id540219/sec2>

Love

- CPR-loven. <https://www.retsinformation.dk/forms/R0710.aspx?id=191719>
- Straffelov Danmark: <https://www.retsinformation.dk/Forms/R0710.aspx?id=202516>
- Straffelov Norge (§ 202 om identitetskrænkelser).
https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_2-6#KAPITTEL_2-6
- Straffelov Holland: <https://wetten.overheid.nl/BWBR0001854/2019-04-01>

Besøgte hjemmesider

Virksomheder, myndigheder mm

- www.affinion.dk
- www.alka.dk
- www.almbrand.dk
- www.basisbank.dk
- www.codan.dk
- www.collectia.dk
- www.cvr.dk
- www.danskkvindesamfund.dk
- www.debito.dk
- www.detailfolk.dk
- www.digst.dk
- www.dkr.dk
- www.ellos.dk
- www.experian.dk
- www.finansdanmark.dk
- www.gjensidige.dk
- www.inkassoadvokat.dk
- www.iom.dk
- www.jm.dk
- www.krisecentrene.dk
- www.kromannreumert.com
- www.les.dk
- www.ligevaerd.dk
- www.nationalbanken.dk

- www.politi.dk
- www.redbarnet.dk
- www.socialeretshjaelp.dk
- www.taenk.dk
- www.topdanmark.dk
- www.tryg.dk

Informationsportaler

- www.borger.dk
- www.forsikringsportalen.dk
- www.sikkerdigital.dk

Journalistik

- www.berlingske.dk
- www.bt.dk
- www.dr.dk
- www.ekstrabladet.dk
- www.information.dk
- www.jyllands-posten.dk
- www.politiken.dk
- www.skivefolkeblad.dk
- www.tv2.dk
- www.zetland.dk

Udenlandske hjemmesider

- www.actionfraud.police.uk
- www.cifas.org.uk
- www.nettvett.no
- www.rijksoverheid.nl/contact/contactgids/centraal-meld-en-informatiepunt-identiteitsfraude-en-fouten-cmi
- www.sbb.no
- www.slettmeg.no

Sociale medier

- Ask
- Facebook
- Instagram
- Google
- Tinder