Kandidatspeciale 2021

AALBORG UNIVERSITET

Kriminalisering af identitetstyveri og identitetsmisbrug i Danmark

Titelblad

Uddannelsesinstitution:	Aalborg Universitet
Uddannelse:	Jura - Department of Law
Eksamen:	Kandidatspeciale – Master thesis
Dansk titel:	Kriminalisering af identitetstyveri og identitetsmisbrug i Danmark
Engelsk titel:	Criminalization of identity theft and identity fraud in Denmark
Retsområde:	Cybercrime og hacking
Afleveringsdato:	19.05.2021
Vejleder:	Birgit Feldtmann
Antal anslag:	143.994
Antal sider:	77

Forfatter Christine Frank Sønnichsen

20196871

Abstract

Cybercrime and targeted hacking attacks are a rising globally issue. As the latest threats in the landscape of cybercrime and hacking appears, the number of cyber threats including phishing, spear phishing and identity theft is rising, and hereby the numbers of identity fraud, when wrongfully obtaining personal data and using another person's personally identifying information causing injury or inconvenience, typically for economic gain. Not only legal figures are being exposed to these types of crimes, but ordinary people are targeted as subject to gain information from.

The issue of phishing has been known for several years, recently spear phishing has arisen, with more tailored impersonations targeting interests with authorized messages that often never fails, but do people recognize when they are been baited, as part of a social engineering, since these cyberattacks often are masqueraded by a trusted source of a reliable sender. And with anonymous criminals using these attacks to gain information on people in order to acquire the identity for illegal purposes - cyberattacks have gone viral - leaving the law protecting individuals from these hackers to be questioned.

Protection aimed at data and information were inserted to the danish criminal code back in 1985. The scope of the provision is unauthorized access, which has gone untested in practice, leaving the courts with a high degree of discretion to determine the scope of the criminalization. Neither identity theft nor identity fraud is a new form of crime, but technology has provided new opportunities and hereby means to carry them out, which contributed the debate if identity theft should be a separate offense in the criminal code.

In Denmark it is not directly criminalized to gain or use information regarding another person's identity, therefor the thesis will analyze the grey area determining when an act can and will become illegal and which remedies are implemented to defend the individuals from being a victim to identity fraud.

The thesis will take a closer look into the danish law and regulations on identity theft comparing it with the regulations in Norway and Sweden, which both have criminalized identity theft with its own provisions, to examine how Denmark is combatting cyber fraud.

The thesis will mainly look at remedies used to combat such crimes as a cyber self-defense to identity theft and to analyze the possibilities of implementing different regulations to increase cybersecurity in this area.

The main purpose of the thesis is to describe the legal situation in Denmark and to analyze the remedies implemented to combat the cyberattacks on identity theft.

Indholdsfortegnelse

Kapitel 1

1.1 Indledning

Cybercrime er et nyere fænomen, der har været voksende i takt med internettets udbredelse. Den it-teknologiske udvikling er hastigt stigende, hvorfor der i stigende grad etableres digitale løsninger. Løsninger, der muliggør flere sårbarheder i takt med, at vi bliver mere og mere afhængige af internettet. Cybercrime er derfor en kriminalitetsform, der er kommet for at blive, og hvert 39 sekund[1] begås et cyberangreb. I år 2015 kostede cyberangreb på verdensplan $3 trillioner (USD)[2]. Et estimat antager, at beløbet stiger til $6 trillioner (USD) i 2021, og $10.5 trillioner (USD) i 2025 med en årlig stigning på 15 pct.[3]. Sammenholder man 'cybercrime' til verdensøkonomien, ville cybercrime i 2021 være verdens tredje største økonomi efter USA og Kina, jf. data fra Nasdaq[4].
Begrebet 'cybercrime' omhandler kriminelle handlinger, som udøves ved brug af et netværk, herunder computer[5] og andre mobile informationsnetværk[6]. Cybercrime oversat til dansk er 'internetkriminalitet'. Det er en udbredt kriminalitetsform i Danmark, idet mange er bekendt med begrebet, da de enten gennem privat- eller erhvervslivet har været offer for denne type kriminalitet. Ser vi nærmere på it-kriminalitet i Danmark, så er Danmark, som et af verdens mest digitaliserede lande[7], særligt udsat. I takt med sårbarheder og antal af cyberangreb stiger, forsøger den danske stat sammen med danske virksomheder at udvikle og forbedre it-sikkerheden. I 2019 oplevede 43 pct. af befolkningen it-sikkerhedsproblemer, og hver tredje virksomhed, 250+ ansatte, oplevede brud på it-sikkerheden, som følge af cybercrime angreb. Angreb, hvoraf hver tiende virksomhed oplevede, at fortrolige oplysninger blev kompromitteret[8].

It-kriminalitet er et vidt begreb, og kategoriseres derfor ofte yderlig for at konkretisere indholdet af handlingerne. Opdelingen kan jf. Det Kriminalpræventive råd[9], inddeles i tre grupperinger: computer-integritetsforbrydelser, assisterede forbrydelser eller indholdsforbrydelser. Dette

[1] Jf. Sangster, Mark: No safe Harbor, side 8
[2] Jf. Cybersecurityventures: Cybercrime To Cost The World $10.5 Trillion Annually By 2025
[3] Jf. Cybersecurityventures: Cybercrime To Cost The World $10.5 Trillion Annually By 2025
[4] Jf. Nasdaq: 5 Largest Economies In The World And Their Growth In 2020
[5] Jf. Udsen, Henrik: IT-ret, side 49f
[6] Jf. European Commission: Cybercrime samt Udsen, Henrik: IT-ret, side 56
[7] Jf. CFCS: Beretning 2019
[8] Jf. Danmarks Statistik: Halvdelen har oplevet it-sikkerhedsproblemer
[9] Jf. Det Kriminalpræventive råd: IT-kriminalitet i tal

kandidatspeciale tager udgangspunkt i de computer-assisterede forbrydelser, der gennem hacking angreb som phishing, ofte har et økonomisk sigte med det formål at begå tyveri eller bedrageri ved hjælp af internetteknologi. Her anvendes teknologien som redskab til at realisere forbrydelser som databedrageri, phishing og identitetstyveri[10].

Hacking er som it-kriminalitet udtryk for, set fra et it-sikkerhedsperspektiv, den udfordring sikkerheden udgør ved et it-system[11]. Det er et vidt defineret begreb, da hacking omhandler alle måder at kompromittere digitale enheder, hvorfor det i kandidatspecialet særligt er phishing og spear phishingangreb, der belyses som del af social engineering (herefter SE).
Begrebet 'phishing' dækker over det, at man gennem SE manipulerer en person, der franarres personlige oplysninger[12] på inficerede filer eller links og falske hjemmesider[13]. Det er et udtryk for, at man gennem manipulation forsøger at omdirigere en bredere målgruppe til en forfalsket hjemmeside, hvor de bliver bedt om at indtaste fortrolige oplysninger med henblik på misbrug. De såkaldte hackere forekommer som en legitim kilde, og derved er individerne ofte i god tro og uvidende om at identitetsoplysningerne er kommet i de forkerte hænder, da hacking angrebet er nøje udformet.
Spear phishing, er en forbedret version af de såkaldte phishingangreb, og omhandler mere organiserede og målrettede angreb til en smallere målgruppe. Der er tale om personificerede angreb, der adresseres direkte til individerne som offergruppe, hvorfra personoplysninger ønskes frataget. Hensigten er at lokke individerne til at oplyse og afgive personidentificerbare oplysninger i god tro. Informationer, der ved denne handling er dem franarret, og som senere kan bruges som led i anden kriminel sammenhæng.

I Danmark har 43 pct. af befolkningen i målgruppen 16-89 år i 2019 været udsat for phishingangreb[14], jf. Bilag 1. Phishing er derfor et aktuelt emne i den kriminelle teknologiske verden. Disse angreb benyttes ofte som indgangsvinkel til at begå anden kriminalitet, herunder identitetstyveri. Identitetstyveri er et bredt begreb. Betegnelsen rummer alt fra ulovlig tilegnelse af

[10] Jf. Det Kriminalpræventive råd: Cybercrime – når kriminaliteten rykker online
[11] Jf. Aalborg Universitet, Lene Wacher Lentz: Hacking forbrydelse eller digitalt selvforsvar, side 78
[12] Jf. Udsen, Henrik: IT-ret, side 341f
[13] Jf. CFCS: Beretning 2019, side 17
[14] Jf. Danmarks Statistik: Halvdelen har oplevet it-sikkerhedsproblemer

identitetsoplysninger til misbrug af disse personlige oplysninger. Det er udtryk for, at andre tilegner sig en anden persons identitet. Dette kan ske gennem offentlige tilgængelige oplysninger eller gennem handlinger, hvor individet bliver franarret sådanne identitetsoplysninger, som senere kan misbruges i en anden kriminel sammenhæng, der ofte har en økonomisk vinding.

Identitetstyveri dækker over begrebet,

1) *at nogen ulovligt tilegner sig en andens oplysninger*, *og/eller*
2) *at nogen misbruger disse oplysninger*[15].

Individerne er ofte uvidende om, at deres personoplysninger er kommet i de forkerte hænder, da tilegnelsen, som altovervejende hovedregel, sker af professionelle kriminelle, der udgiver sig som legitim kilde. Det er først ved senere realiseret kriminalitet, at ofrene bliver bekendt med handlingerne, og at de er offer for identitetstyveri, da deres personoplysningerne herved bliver misbrugt. I den sammenhæng kan begrebet identitetsmisbrug være nærliggende at benytte, da ofrene først i takt med en begået forbrydelse bliver bekendt med de begåede handlinger, som identitetstyveriet har medført. Alt i alt dækker begrebet dermed over handlinger, hvor individets identitet er franarret til brug i anden it-kriminel sammenhæng, som ofte først ved en reel fuldbyrdelse af en forbrydelse, nærmere gennem misbrug af oplysningerne, opdages. Idet identitetstyveri ikke er et særskilt juridisk begreb, kan det medføre forvirring omkring begrebsdefinitionen, hvorfor der henvises til en mere dybdegående analyse i kapitel 2.

Som nævnt benyttes identitetstyveri ofte som forudgående led til anden it-kriminalitet. Det kan være hensigten at begå chikane, tyveri eller bedrage personer ved hjælp af de ihændehavende identitetsoplysninger. Fællesnævneren er ofte en økonomisk vinding, som dette speciale tager udgangspunkt i.

Kriminalstatistikken viser, at der i år 2010 var 1.336 anmeldelser om databedrageri, samt hele 22.467 anmeldelser i år 2019, hvilket er en stigning på 17 gange. Databedrageri udgør nu 46 pct. af

[15] Jf. Borger.dk: Hvad er identitetstyveri

de samlede anmeldelser af bedrageri[16], hvilket er tydelige tegn på, at it-kriminalitet er i fremgang samtidig med, at samfundet bliver mere og mere afhængige af den digitale verden. En stigning i cybercrime har medført en stigning i identitetstyveri, hvor en person bruger en andens identitet til at forårsage skade eller gener for den pågældende. De kriminelle hackere kan være alt fra professionelle aktører til private borgere, og det kan derfor være svært at definere. I internationale it-sikkerhedskredse sondres ofte mellem tre forskellige typer hackere. Black-hat-hackere, som begår en forbrydelse og bliver strafansvarlige. Modsætningsvis er white-hat-hackere, som etiske hackere med et legitimt formål som at teste it-sikkerheden,[17] og til sidst sondres gråzonen mellem black- og white-hat-hackere, og betegnes grey-hat-hackere. Grey-hat-hackere kan agere ud fra meget forskellige motiver[18]. Deres adfærd kan derfor være problematisk, og i nogen tilfælde kan de ifalde strafansvar efter den danske straffelov. I dette kandidatspeciale, vil disse typer hackere kort belyses i forhold til forsæt i forhold til strafpålæggelse, og til at belyse om forsæt har betydning i forhold til strafpålæggelsen, se nærmere kapitel 3. Endvidere er det min antagelse at COVID-19 pandemien har gjort markedet for cybercrime mere sårbart, særligt også udbredt identitetstyveri, hvorfor denne antagelse vurderes i forhold til retstilstanden i kapitel 5.

For at regulere it-kriminalitet i Danmark er der nedsat specialenheder indenfor cybercrime, herunder er Cybersikkerhedsrådet etableret i 2019. Rådet består af Digitaliseringstyrelsen og Center for Cybersikkerhed (CFCS). Dertil er der også tiltag som Center for Cyberkriminalitet og Cybersikkerhed (CCC), som er med til at fremme beskyttelsesniveauer og understøtte lovgivningen i Danmark. Cybercrime behandles i Danmark af politiets NC3 gruppe, som er rigspolitiets nationale Cyber Crime Center. Ellers er problemstillingen underlagt Finansministeriet, der gennem Digitaliseringsstyrelsen har til opgave at fremme informationssikkerheden. De strafbare handlinger inden for identitetstyveri reguleres hovedsageligt i straffelovens specielle del (herefter STRFL), og gennem kandidatspecialet vil disse bestemmelser belyses, så de nærmere rammer for strafpålæggelse kan fastlægges i forhold til regulering af identitetstyveri.

I kommende kandidatspeciale vil 'hackeren' bliver brugt som den fjendtlige angriber, hvor 'it-

[16] Jf. Danmarks Statistik: Stigning I anmeldt bedrageri
[17] Jf. A. Gillespie, Alisdair: Cybercrime – Key Issues and Debates, side 29
[18] Jf. Malwarefox: Types of Hackers You Should Know

aktørerne', er det it-system, herunder den virksomhed eller privat person, som er offer for et cyberangreb, og endvidere vil begrebet individ/'individerne' benyttes, som betegnelse for ofrene for identitetstyveri.

1.2 Problemformulering

Kandidatspecialet analyserer kriminalisering af identitetstyveri og identitetsmisbrug. I den sammenhæng inddrages en analyse af eventuelle uklarheder i det strafferetlige værn, og problemstillingen sammenholdes med regulering af identitetstyveri i norsk og svensk strafferet for at vurdere retstilstanden i Danmark.

1.3 Afgrænsning

Da kandidatspecialet omhandler hacking, vil det kunne give anledning til en større analyse af jurisdiktion, en analyse som ikke er medtaget grundet omfang af kandidatspecialets størrelse.

Kandidatspecialet forsøger at indramme kriminalisering af identitetstyveri, og afgrænses derfor til at omhandle denne konkrete type hacking angreb, hvorfor andre aspekter af bestemmelserne i STRFL §§ 21, 23, 171, 263, 276 279, 279a hovedsageligt kun behandles i lyset af denne problemstilling. Endvidere er typerne af identitetsmisbrug ikke nærmere beskrevet, da retsgrundlaget har været i fokus, og kandidatspecialet vil derfor ikke konkret behandle en dybere analyse af identitetstyveri typerne (så som æreskrænkelser, identitetskloning, økonomisk- eller medicinalt identitetstyveri til syntetisk identitetsmisbrug mv.). Alt overvejende er det den økonomiske vinding, som danner grundlag for de kriminelle handlinger, hvorfor der er taget udgangspunkt i denne hensigt gennem opgaven. Hovedsageligt er det de online aktiviteter, som gennem kandidatspecialet vil blive belyst, hvorfor disse handlinger primært er anvendt i analysen. Andre eksempler er alene medtaget for at underbygge forståelse af retstilstanden med den foreliggende retspraksis.

Desuden dækker misbrug af identitetsoplysninger ikke over misbrug af kreditkortoplysninger[19] i dansk ret, jf. Kriminalpræventive Råd[20] samt Digitaliseringsstyrelsens definition, hvorfor denne handling ej nærmere er belyst.

Endvidere behandler kandidatspecialet ikke en gennemgang af alle former for cybercrime angreb inden for identitetstyveri, da det vil være for vidtgående at beskrive alt fra hacking, malware, spyware, randsomware, DDoS-angreb, spoofing, spam, mv. Listen over typer af cybercrime er lang, og derfor er det i kandidatspecialet afgrænset til at omhandle SE jf. bilag 2, herunder er særligt phishing og spear phishingangreb anvendt, som værende de mest omfattende og mest aktuelle.

Da hacking omhandler data, særligt personoplysninger, til brug for identitetstyveri og identitetsmisbrug, som omfattes af persondataloven, afgrænses kandidatspecialet til ikke at omhandle det eventuelle strafansvar ved uberettiget anvendelse af persondata, hvorfor persondataloven (GDPR) ikke nærmere er anvendt.

1.4 Retskilder og Metode

I kandidatspecialet er det primært den nationale lovgivning i form af straffelovens specielle del, herunder § 263 bedre kendt som hacking bestemmelsen, § 279 om bedrageri og § 279a om databedrageri, samt §§ 171 og 276, om henholdsvis dokumentfalsk og tyveri, som de mest centrale bestemmelser, der danner grundlag for opgaven. Bestemmelserne sammenholdes med den norske straffelov Lov om straff (herefter strl.) kapittel 21 vern av informasjon og informasjonsutveksling § 202 og svensk straffelov Brottsbalk (herefter BrB) om olovlig identitetanvändning kapitel 4, særligt § 6 b for at vurdere retstilstanden i Danmark.

1.4.1 Retskilder

Hovedsagligt er national ret brugt som retskilde, herunder retspraksis, forarbejderne og lovforslag. Da Cybercrime er et nyere fænomen, og kriminaliseringen ikke er konkretiseret gennem en bredere

[19] Jf. Borger.dk: Hvad er identitetstyveri
[20] Jf. Kriminalpræventive Råd: Hvad er It-kriminalitet

domspraksis, har det ikke været muligt at bygge en analyse op omkring retsvirkningen af domme sammenholdt med gældende ret. Emnet belyses derfor i form af en komparativ analyse af retstilstanden med inddragelse af anden faglitteratur som samfundsvidenskabelig empiri til at vurdere emnet mere konkret og nutidig.

1.4.2 Retsdogmatisk metode

Kandidatspecialet benytter hovedsageligt den retsdogmatiske metode, som belyser forskellen mellem juridisk teori og praksis, da *den analyserer og beskriver gældende ret* og hermed *retsvidenskab, som beskæftiger sig med den i samtiden gældende ret*[21]. Retsdogmatikken gør brug af juridisk metode gennem valg af retskilder, faktum, fortolkning og resultat[22], hvorfor det vil afspejles i måden fortolkningsprincipperne er anvendt. Den primære retskilde og undersøgelsesobjektet vil være den gældende lov, hvoraf retspraksis er udtryk for gældende ret. Til besvarelse af kandidatspecialets problemformulering anvendes supplerende forarbejder med bemærkninger som supplement til fortolkning af indholdet, og til afvejning af hensyn om bestemmelserne med formålet at beskrive og finde ny viden i henhold til retstilstanden om den gældende ret inden for identitetstyveri og identitetsmisbrug. Det er de retlige begreber, som kvalificeres under virkelighedens fænomener og rammer, som er den egentlige retlige sumption - her er det efter retsdogmatikken vigtig, at intet relevant kildemateriale undlades, og at der særligt stilles kritisk over for kildematerialets anvendelse til at belyse problemstillingen[23].

1.4.3 Komparativ ret

For at danne et mere retvisende billede af det strafferetlige værn i Danmark er en komparativ analyse af udenlandsk national ret anvendt sammen med retsdogmatikken med henblik på at konkretisere og beskrive retstilstanden. Formålet er at belyse virkningen af andre tiltag for at vurdere den danske retstilstand gennem kriminalisering af identitetstyveri og identitetsmisbrug. Denne analyse har særlig fokus på det skandinaviske retsområde, og inddrager her de norske og svenske tiltag for at klarlægge og fortolke anvendelsen af retspraksis i sammenspil med det danske retssystem. Den udenlandske ret er ikke en umiddelbar retskilde, men bruges som inspiration og

[21] Jf. Munk-Hansen. Carsten: Retsvidenskabsteori, side 64
[22] Jf. Munk-Hansen, Carsten: Retsvidenskabsteori, side 204f
[23] Jf. Munk-Hansen, Carsten: Retsvidenskabsteori, side 67

perspektivering til forståelse af den danske retspraksis. Dette er forsøgt udledt gennem en analytisk metode til at belyse retstillingen mere dybdegående end en kortfattet overfladisk Länderbericht-metode[24].

1.5 Udfordringer grundet COVID-19

COVID-19 pandemien har haft indflydelse på alle parametre, og har derfor også haft indvirkning på dette kandidatspeciale. Særligt har det besværliggjort muligheden for at benytte sig af faglitteratur, da bibliotekerne har været lukket. Udlån af bøger har ikke været tilgængelige, hvorfor der er søgt brug af anden såvel dansk som international litteratur, for bedst muligt at have en bred forståelse af emnet. Problematikken har generelt været tilgængeligheden af retskilder og litteratur. Særligt har det været en udfordring at modtage materialer over landegrænserne. Ikke kun den danske litteratur har været længe om at blive leveret, det samme gælder de engelsk trykte bøger, da nedlukning har mindsket effektiviteten og forlænget leveringstiden, samtidig med at toldproceduren over landegrænsen har været forlænget. Desuden har der været problemer med Karnov-adgang, hvilket har besværlig gjort brugen af databasen under speciale skrivning. Yderlig bemærkes kort, at datamateriale benævnt i kandidatspecialet tager udgangspunkt i de nyeste foreliggende datasæt, som ved udfærdigelse af kandidatspecialet foreligger. Det Kriminalpræventive Råd oplyser, at rapporterne for 2020 endnu ikke er offentliggjort, og henviser til datasæt for året 2019, som blev udgivet slut 2020.

Kapitel 2

2.1 Begrebet identitetstyveri

I Danmark er identitetstyveri et begreb som ofte anvendes, dog har det ikke en særskilt juridisk definition. Det har de seneste år været til debat, hvorvidt det selvstændigt bør kriminaliseres i straffeloven. Flere og flere udsættes for it-kriminalitet, men grundet manglende definition og kriminalisering er det svært at klarlægge i hvor høj grad den danske befolkning konkret udsættes

[24] Jf. Munk-Hansen, Carsten: Retsvidenskabsteori, side 72

for identitetstyveri. Der må grundet manglende registrering formodes at foreligge et større mørketal af de kriminelle handlinger, da der ikke forefindes en særskilt gerningskode til anmeldelse af identitetstyveri hos politiet[25]. Hvorfor de benævnte handlinger kun sjældent benævnes, og derfor mere konkret findes under andre gerningskoder, som bedrageri og tyveri, jf. STRFL §§ 279 og 276.
Da Danmarks Statistik ikke ligger inde med alle oplysninger om identitetstyveri, følges deres henvisning til Det Kriminalpræventive råd, der har udgivet talrige rapporter om omfanget af it-kriminalitet. De oplyser at der i år 2017 har været 38.500 tilfælde af identitetsmisbrug[26], og at 10 pct. af befolkningen i 2019 har været udsat for it-kriminalitet, hvilket er en stigning på 8 pct. i forhold til år 2018. Af de foreliggende data har 4 pct. af befolkningen været udsat for identitetstyveri i 2019, men hvad er definitionen af identitetstyveri?

Identitetstyveri dækker over begrebet,

1) *at nogen ulovligt tilegner sig en andens personlige oplysninger*, *og/eller*
2) *at nogen misbruger disse oplysninger[27].*

Således dækker begrebet i første led over selve tilegnelsen af identitetsoplysninger, hvormed andet led, i begrebsdefinitionen, beskriver den efterfølgende ageren, herunder de efterfølgende handlinger, som hackeren benytter personoplysningerne til.
Informationer kan komme en anden i hænde ved at de frit tilgængeligt foreligger i offentligt forum. Samtidig kan der være tale om oplysninger, som fratages gennem hacking eller tyveri, som henholdsvis reguleres i STRFL §§ 263 og 276. Ofte har disse handlinger afsæt i en økonomisk vinding, og hensigten med tilegnelsen af identitetsoplysningerne er derfor ofte med forsæt til at begå anden kriminalitet, så som banksvig, skattesvig, svindel mv. Herunder efterfølgende handlinger hvorpå en hacker kan ifalde straf efter STRFL §§ 279 og 171, nærliggende om bedrageri og dokumentfalsk.
Begrebsdefinitionen beskriver herved to led, der hver tager afsæt i forskellige kriminelle handlinger, hvorfor denne opdeling vil være gennemgående ved analyse af straffelovens bestemmelser, se nærmere kapitel 3.

[25] Jf. Det Kriminalpræventive råd: Faktaark om identitetstyveri
[26] Jf. Det Juridiske Fakultet, Københavns Universitet, Internet Kriminalitet 2017
[27] Jf. Borger.dk: Hvad er identitetstyveri

Definitionen af identitetstyveri er ikke entydig, men danner grundlag for en international anerkendt betegnelse af begrebet. Begrebet omhandler konkret det, at en person anvender personlige oplysninger om en anden til at begå en svigagtig handling, såsom at misbruge den, jf. Economic Co-operation and Development (hereafter OECD) beskrivelse af identitetstyveri:*" occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes*. [28]". Der foreligger ingen konsensus af begrebet, hvorfor der i kandidatspecialet tages udgangspunkt i denne benævnelse, da den fremkommer som værende den internationalt anerkendte betegnelse, som både beskriver tilegnelse af identitetsoplysninger samt misbrug til at begå andre forbrydelser, herunder kriminelle handlinger, som at købe ting, optage lån og snyde andre i handel eller udføre chikane, jf. Digitaliseringsstyrelsens begrebsanvendelse. Det omhandler identitetsoplysninger, særligt personfølsomme persondata, cpr-nummer, adgangskoder eller sundhedsoplysninger, som ofte tilegnes gennem phishing mails, hvor brugeren manipuleres til logge ind på en falsk hjemmeside og dermed egenhændigt oplyser eller videregiver sine identificerbare persondata.

Begrebet identitetstyveri kan skabe forvirring og juridisk set være misvisende, da det giver udtryk for, at man ejer sin identitet på samme måde som en anden materiel genstand, som i givet fald kan stjæles eller fratages denne person. Begrebsdefinitionen kan skabe forvirring om en identitet reelt kan borttages for at skaffe sig uberettiget vinding ved tilegnelsen. Sammenholdes begrebet med tyveribestemmelsen i STRFL § 276, som beskriver en handling, der uden besidderen samtykke fratager en fremmed rørlig ting, vil identiteten fremstå som en genstand, hvilket skaber forvirring, da borttagelsen af oplysningerne, og "selve identiteten", ikke altid sker ved bevidsthed. Hvorfor individerne, som ofre, ikke altid er bekendt med, at deres identitet er frataget og misbruges i anden sammenhæng. Dette kan skabe tvivl, om identiteten kan indgå som en materiel genstand, der efter strafbestemmelsens ordlyd kan fratages, hvorfor denne sondring mere dybdegående vil blive belyst i afsnit 3.2.2.

[28] Jf. OECD: Scoping Paper on Online Identity Theft, side 3

Som kort benævnt i kapitel 1 og 2 er der i sagens natur et stort mørketal, og omfanget af identitetstyveri er derfor ukendt, da det kun er de tilfælde af identitetstyveri, som opfanges, der reelt kan rapporteres og efterforskes. Deraf følger, at der kun er få digitale hacking spor som efterforskes, idet det kun er de indrapporterede forhold, som konkret af forurettede anmeldes, der gennem retsinstansen kan efterforskes, jf. princip om privat og offentlige påtale efter begæring[29], jf. STRFL § 275. Hvorfor begrebet 'identitetsmisbrug' kan virke mere retvisende, idet offeret bliver bekendt med at identitetsoplysningerne misbruges, og dermed rapporterer det, hvormed denne begrebsdefinition kan virke mere konkret og ordlyden mere omfattende, da man undgår at skulle definere selve fratagelsen af identiteten, og definitionen nærmere omhandler de efterfølgende handlinger, som besiddelsen benytter identitetsoplysninger til.

Da kandidatspecialet tager udgangspunkt i ovennævnte begrebsdefinition, vil det gennem specialet være begge udtryk, som benyttes. Identitetstyveri omfatter efter ordlyden mere nærliggende første led af begrebsdefinitionen, hvorunder identitetsmisbrug, som supplement sammenholder andet led. Da begrebsdefinitionen for kandidatspecialet er defineret, bringer det os videre til næste afsnit og hermed den egentlige analyse af retstilstanden i Danmark.

Kapitel 3

3.1 Regulering af identitetstyveri i Danmark

Ser vi nærmere på retstilstanden i Danmark, er det en grundlæggende forudsætning, at der er sket en forbrydelse, for at man kan ifalde straf. Der er således et krav om lovhjemmel, jf. legalitetsprincippet, jf. STRFL § 1, idet ingen kan straffes for en handling, som ikke er defineret som en overtrædelse af gældende lov, da man skal have muligheden for at overveje den pågældende handling i forhold til en eventuel straf for overtrædelsen. Når det grundlæggende med en lovbestemmelse er på plads, ser vi nærmere på de almindelige strafbarhedsbetingelser, her hvilke led i bestemmelsen, der kræves opfyldt eller hvilke elementer, der skal være til stede, før man kan ifalde straf for den pågældende overtrædelse. Herunder at realisere et gerningsindhold og sikre at

[29] Betænkning nr. 1563 af 2017 om freds- og æreskrænkelser, side 17

leddene under stafbestemmelsen er opfyldt i et bestemt gerningsindhold, som således skal matche strafbestemmelsen. Såfremt handlingen ikke 'matcher' en eksisterende strafbestemmelse, kan man ikke dømmes herfor[30]. Der stilles ikke kun krav til gerningsindholdet, men også at gerningsmanden har det pågældende forsæt. Hovedreglen er, at gerningsmanden skal have forsæt under forbrydelsen eller hvad der kan henregnes, herunder at handle med det fornødne forsæt. I speciellovgivningen er en *uagtsomhed* tilstrækkelig til at statuere et sådant forsæt.

For at undersøge retstilstanden for kriminalisering af identitetstyveri, må vi først udlede beskyttelsesobjektet efter straffeloven, for dernæst at definere det nærmere indhold og rammerne for strafpålæggelse efter de enkelte strafbestemmelser i den gældende straffelov.

Den traditionelle privatlivsbeskyttelse kan tilføres til 1866, hvor kernen af straffeloven med privatlivets fred gennem en beskyttelse af brevhemmeligheden blev indsat[31]. I 1980'erne blev man opmærksom på datamaskiner som nyt værktøj til at begå kriminalitet, ligesom det kunne blive genstand for kriminalitet[32]. Hvorfor man ved Lov 1985-060-06 nr. 229, omhandlede datakriminalitet, foretog ændringer i STRFL og indsatte nye beskyttelsesobjekter og tilsigtede en sikring af databehandling i straffelovens § 263 om hacking, samt bedrageri, her særligt databedrageri i STRFL § 279a. Beskyttelsesobjektet 'oplysninger' samt virkning af daværende datamaskiner blev derfor for første gang indsat i straffeloven. I takt med den teknologiske udvikling har beskyttelsesinteressen fået en videre betragtning. Æreskrænkelser er fortsat baseret på den mere traditionelle tilgang, hvor hensynet under fredskrænkelser ikke kun omhandler privatlivet i snæver forstand[33], men har de senere år skabt og tilsigtet en videre beskyttelse i takt med teknologiens udvikling, da virkeligheden, hvorpå de kriminelle handlinger sker ikke kun begrænses til den fysiske verden. Indtil 80'erne mente man ikke at maskiner kunne være led eller genstand i en forbrydelse, og dermed agere som den automatiserede proces til at forårsage vildfarelse efter STRFL § 279. Derfor blev en ny strafbestemmelse med STRFL § 279a indsat til at belyse denne manglende

[30] Jf. Trzaskowski, Jan: Internetretten, side 578
[31] Jf. Trzaskowski, Jan: Internetretten, side 589
[32] Jf. Trzaskowski, Jan: Internetretten, side 575
[33] Jf. Toftegaard Nielsen, Gorm: Kommenteret straffelov, side 501

kriminalisering. Beskyttelsesobjektet er derfor blevet mere praktisk relevant og rummer meget forskelligartede handlinger med en vidtgående ordlyd og dermed en vidtgående kriminalisering.

Et anmeldt identitetstyveri vil alt efter omfang og alt efter fremgangsmåde kunne straffes efter STRFL §§ 171, 263, 276, 279[34]. Som udgangspunkt gælder de samme strafferetlige overvejelser i forhold til it-kriminalitet i virtuelle rum, som overvejelser der i den fysiske verden efter gerningsindhold statuerer ansvar. Et eksempel herpå er videregivelse af oplysninger. Det har derfor ikke betydning om dokumenterne videregives i den fysiske eller virtuelle verden, da det er selve handlingen, som er kriminaliseret og herved selve videregivelsen af oplysninger, som forlanges unddraget for bredere offentlighed, jf. STRFL § 264 d.

Af ovenstående er rammerne for beskyttelsesobjektet nærmere defineret, hvilket bringer os videre til den egentlige analyse af det strafferetlige værn for identitetstyveri. Idet, identitetstyveri, i dansk ret, ikke er selvstændig kriminaliseret vil rammerne for strafpålæggelse i kommende afsnit blive belyst i forhold til de enkelte delikter i henholdsvis STRFL §§ 263, 276, 171 og dernæst § 279. Først vil de enkelte led i begrebsdefinitionen introduceres, og dernæst vil analysen bygge på en mere dybdegående gennemgang af de enkelte strafbestemmelser med henblik på at belyse de enkelte kendetegn i forhold til en strafferetlig regulering og kriminalisering af henholdsvis identitetstyveri og identitetsmisbrug.

3.2 Tilegnelse af identitetsoplysninger

Begrebsdefinitionen af identitetstyveri vedrører i første led den måde, hvorpå selve identitetsoplysningerne kommer hackeren i hænde. I den fysiske verden kan der være tilfælde, hvor persondata og andre personfølsomme oplysninger ligger frit tilgængeligt i offentlige rum. Det samme gælder i virtuelle rum, hvor oplysninger kan foreligge på offentlige profiler eller være delt gennem oplæg. Sondringen vil derfor være om identitetsoplysningerne fremstår frit på offentlige hjemmesider, eller om der er tale om en nærmere privat side, hvorfor informationen synes unddraget en bredere offentlighed. Endvidere bygger sondringen særligt på, om fratagelsen sker på

[34] Jf. Det Kriminalpræventive råd: Faktaark om identitetstyveri samt Borger.dk: Offer for identitetstyveri

baggrund af samtykke, eller om det vedrører en uberettiget fratagelse eller tilegnelse. Hvorfor det i dette afsnit særligt er måden, hvorpå identitetsoplysningerne kommer identitetstyven i hænde, som er afgørende for hvilken strafbestemmelse, der kan dømmes efter, da det er udslagsgivende for den efterfølgende retsvirkning.

På den ene side kan oplysningerne blive fremlagt af individet selv, herved benævnt, at individet egenhændigt videregiver oplysningerne til sine nærmeste eller uagtsomt efterlader personfølsomme oplysninger frit tilgængelig. På den anden side kan der være tale om en fratagelse af oplysninger, der sker gennem aktive handlinger eller manipulation, hvorfor der er tale om, at oplysningerne, uden individets samtykke eller direkte kendskab, kan blive stjålet og dermed frataget. De benævnte handlinger kan ske online, men også offline, hvorfor dette kandidatspeciale hovedsageligt afgrænses til at rumme de kriminelle handlinger online. Da retspraksis på området er minimal i forhold til identitetstyveri, vil sondringen til andre sammenhænge benyttes for at belyse gerningsindholdet bedst muligt.

3.2.1 Hacking, jf. straffelovens § 263

STRFL § 263 er kendt som hackingbestemmelsen. Strafbestemmelsen er en del af straffelovens kapitel 27 omkring freds- og æreskrænkelser, og omhandler krænkelser af privatlivets fred. Beskyttelsesobjektet i kapitel 27 har fået en videre betragtning i takt med den teknologiske udvikling, hvormed brevhemmeligheden og dermed en lukket meddelelse efter fortegnelse nu også rummer meddelelser i elektronisk form.

Hackingbestemmelsen straffer den, *der uberettiget skaffer sig adgang til en andens datasystem eller data*, *som er bestemt til at bruges i et datasystem*. Gerningsmanden kan derfor ifalde straf på 1 år og 6 måneder. Hvis man, som hacker, opnår kendskab til oplysninger eller programmer gennem hacking, kunne strafbestemmelsen i STRFL § 263, stk. 1, nr. 1 være anvendt, men for at præcisere strafbarheden er § 263, stk. 2 indsat med præcisering af en 'uberettiget' adgang (unauthorised access)[35]. For at præcisere nogle af disse begreber, og hvad der konkret forstås med *'uberettiget'*, navnlig en *uberettiget adgang til andens oplysninger eller programmer*, herunder

[35] Jf. Richardson, Matthew: Cybercrime – Law and Practice, side 7

informationssystemer og hvad der anses for ensbetydende med data, vil som selvstændig begreb først beskrives.

Begrebet 'data'*, forstås om enhver form for repræsentation af kendsgerninger eller ideer, der kan kommunikereres eller behandles gennem en eller anden proces*[36].

Betingelsen er, at oplysningerne eller programmet skal være "en andens", og det at skaffe sig uberettiget adgang til disse oplysninger er den strafbare handling efter gerningsindholdet, hvorfor stk. 2 er indsat for at synliggøre strafbarheden. Hacking benyttes ofte som indgangsvinkel til at begå identitetstyveri, og strafbestemmelsen kriminaliserer den, som *skaffer sig adgang* til data eller programmer i datasystemet. Data- eller informationssystemer omfatter også mobiltelefoner og andre servere, der kan udføre samme funktioner, svarede til en computer. Rammerne er derfor brede, og strafbestemmelsen indrammer såvel det at logge på en andens computer uden hjælp af hackerværktøj, som det at skaffe sig adgang til denne ved brug af hackerangreb og hackerværktøj.

Det angives med ordet *uberettiget,* at det ikke henfører enhver handling, som er strafbar, hvorfor en white-hat-hacker ville have den pågældende hjemmel til at hacke sig ind i IT-aktørens system, da denne hacker har en legitim og dermed berettiget adgang. Problematikken opstår her, hvis hackeren tilgår systemer, som man ikke er berettiget til. Det tager derfor udgangspunkt i det samtykke, man fra systemejeren har fået, og dernæst om denne adgang er berettiget eller uberettiget[37], hvorfor tiltalte i U.1996.979 Ø blev frifundet, da han på tidspunktet for tilgang til systemet var ansat, og ved anvendelse af egen password havde en berettiget adgang.

Bestemmelsen i STRFL § 263 angående fredskrænkelser kræver forsæt for at ifalde strafansvar, og en vildfarelse diskulperer. Forsæt mangler, såfremt hackeren ved god tro har regnet med samtykke til brugen eller ikke har haft forsæt og haft henblik på, at personerne kunne identificeres[38]. Endvidere gælder det, at man inden for rammerne ikke kan fritages for straf, hvis man uberettiget får adgang til et system, trods hensigten er at teste systemet, finde en systemfejl, eller sikkerhedsbrist i legitimt formål. Hackeren har i dette tilfælde begået den efter STRFL § 263 strafbare handling ved uberettiget at skaffe sig en adgang, som ikke kan fritages for straf.

[36] Jf. Toftegaard Nielsen, Gorm: Kommenteret straffelov, side 507
[37] Jf. Trzaskowski, Jan: Internetretten, side 595
[38] Jf. Waaben, Knud: Strafferettens specielle del, side 237

Det kan endvidere være svært at håndhæve, hvornår en handling forfølger et legitimt formål, og yderlig vil denne mulige undtagelse eller straffrihed nærliggende statuere en nem udvej for, at hackere ikke ifalder straf. Hvorfor man kan udlede, at det i det danske retssystem mere konkret omhandler sondringen om et legitimt samtykke til den pågældende handling, dernæst om der er tale om formildende omstændigheder, hvis formålet vedrører en gråzone. Handlingen, nærmere bestemt det at skaffe sig adgang til noget, der med rimelighed kan forventes lukket eller utilgængeligt, straffes med bøde eller fængsel i op til 1 år og 6 måneder. Såfremt gerningen ikke er omfattet af stk. 1., men at man uberettiget gør sig bekendt med indholdet eller aflytter, vil der kunne straffes med bøde eller fængsel indtil 6 måneder, jf. stk. 2.
Stk. 3. sigter særligt mod erhvervsspionage, men kriminaliserer også andre skærpende omstændigheder, her udtrykkeligt hacking angreb, der har karakter af systematisk og organiseret aktiviteter, hvilket kan være et strafforhøjende element med fængsel op til 6 år.

I strafbestemmelsen afvejes hensyn, hvor hensynet på den ene side angår IT-aktørerne, som tillader adgang til systemerne, modsat hensyn til brugerne og individerne af platformene, der herunder af internettet, som helhed, forventer frit og anonymt at kunne søge informationer. Hvorfor hacking som altovervejende hovedregel kræver hjemmel og dermed en legitim adgang til it-systemet. Såfremt man egenhændigt tilegner sig adgang til et system, risikerer man straf. Som beskrevet findes der forskellige typer hackere, og problematikken opstår, hvis man anser sig selv som white-hat-hacker, der med rette tilgang har adgang til systemet og de personidentificerbare oplysninger, hvorfor de nok mere retvisende må betegnes grey-hat-hackere, da deres adfærd er problematisk, idet de uden adgang har tilegnet sig adgang til et system og dermed oplysninger om de pågældende personer. Grey-hat-hackere risikerer dermed at ifalde straf, idet det strafbare forhold ikke forudsætter, at man har gjort sig bekendt med oplysningerne, men alene straffer handlingen *at skaffe sig adgang*.

Kandidatspecialet har til sigte at belyse kriminaliseringen, og fokus vil derfor være på den uberettiget tilegnelse af personoplysninger, dermed en tilegnelse, som er sket uden samtykke fra it-aktøren eller individet selv, med henblik på at definere det strafferetlige værn mod

identitetstyveri. Tilegnelse kan ske som følge af SE-angreb, der ofte har til hensigt at skaffe sig en uberettiget økonomisk vinding ved bedrageri og manipulation.

For at sondre om der er tale om en uberettiget adgang, eller på den anden side oplysninger, der er tilgængelige, må man afveje hensyn. Det er op til en sondring af den konkrete sag, da man ikke kan ligestille online aktiviteter på samme måde som med fysiske objekter. Hvorfor en webserver, der er frit tilgængelig ikke kan sidestilles med en skrivebordsskuffe, særligt fordi det modsatte hensyn gør sig gældende ved at informationerne ligger i en skuffe, ulåst eller ej, idet det ikke anses som tilgængelig.[39] I U.2020.4282, havde forurettede A kortvarigt givet tiltalte (herefter T) adgang til identitetsoplysninger for at få hjælp til spærring af kort. T havde efterfølgende optaget lån i A's navn og samtidig flyttet bankkonti og dermed uberettiget handlet i A's navn. Tager man udgangspunkt, at individet selv har fremlagt oplysninger i offentligt rum, er der ikke tale om at disse oplyser direkte stjæles eller franarres. Såfremt personen selv ved uagtsomhed har videregivet identitetsoplysninger, vil man nærmere se på de efterfølgende handlinger og en uberettiget brug af disse oplysninger, se nærmere afsnit 3.3.

Er det omvendt tale om, at oplysningerne franarres individet, vil det i det virtuelle rum ofte omhandle hacking og hermed tyveri af identitetsoplysningerne, hvorfor identitetstyven alt efter omfang kan ifalde straf som følger i pågældende sager. En international velkendt sag er den omtalte MySpace-sag, hvor hackerne gennem phishingangreb fik individerne til at installere "MySpace Profile Object" for at tilgå deres profil. Dette alene for at installere to trojanske heste med henblik på at indsamle oplysninger om den gældende person til senere brug af identitetstyveri[40], hvilket også skete for Nordea samme år. Endvidere blev CSC i 2012 udsat for hacking. En sag som siden er kendt, som den "største hacking" sag i Danmark[41], hvorved flere filer herunder CPR-registeret samt politiets registre blev downloadet. Tiltalte (herefter T) fik herved adgang til informationer i et ikke tilgængeligt offentligt system og dermed en uberettiget adgang, hvorfor betingelsen om "*uberettiget*" utvivlsomt var opfyldt, hvorfor T i sagen blev idømt 3,5 års fængsel. Løbende er en række danskere blevet udsat for hacking. Her kan i år 2008 benævnes en sag, hvor borgerne fik

[39] Jf. Trzaskowski, Jan: Internetretten, side 597
[40] Jf. Trzaskowski, Jan: Internetretten, side 614
[41] Jf. CSC- sagen - U.2015.3615Ø, jf. Trzaskowski, Jan: Internetretten, side 592

tilsendt mails, såkaldte phishing mails, med henvisning til at opdatere konti med oplysninger, herunder tilknytte betalingskort for at modtage bonuspoint[42]. *Phishing,* er et nyere fænomen, der ofte anvendes som underkategori i forlængelse af identitetstyveri, hvor hackeren forsøger at franarre oplysninger fra individerne ved at tilsende en mail med tilhørende link i forsøg på at få brugeren til at indsende oplysningerne, herunder særligt loginoplysninger ved at logge ind på forfalsket hacker/phishing-hjemmeside, som ligner denne IT-aktørerne normalt bruger[43]. Phishing er dog ikke begrænset til e-mails, men er udbredt til også at omhandle SMS-beskeder, også kaldet *smishing[44]*. Større organisationer, som benævnt, MySpace og Nordea, har været udsat for sådanne phishingangreb, og hele 43 pct. af den danske befolkning har i 2020 modtaget phishing mails, hvoraf 3 pct. direkte har mistet penge, som følge heraf[45].

Det kan af ovenstående udledes, at databedrageri er i progressiv stigning særligt set i lyset af den teknologiske udvikling de seneste år, jf. bilag 3, bilag 4 samt bilag 5. Phishingangreb er, som betegnelsen udtrykker, en succesful måde at tilegne sig identitetsoplysninger om individer. I takt med udvikling og hackernes dygtiggørelse, har disse hacking angreb og teknikker også udviklet sig. En videreudvikling af phishingangreb er *spear phishing*, der de seneste år haft en progressiv stigning. Begrebet definerer de personificerede og mere målrettede adresserede cyberangreb, hvor fejlraten er meget lav og dermed endnu lavere end phishingangreb. Der er her tale om e-mails, der detaljeret rettes mod en bestemt person eller organisation og dermed en nøje udvalgt målgruppe, hvilket også er udtryk for, at disse angreb sjældent fejler. Som nævnt er disse hacking angreb kun en brøkdel af de mulige trusler verdenssamfundet står over for, særligt i forhold til identitetstyveri.

For at klarlægge retspraksis i forhold til identitetstyveri tages udgangspunkt i en række domme for at belyse nogle af straframmerne. Interessant er sondringen, hvornår noget er rimeligt unddraget offentligheden, da der ikke stilles klare rammer hertil. I sagen af U.2017.247V blev tiltalte (herefter T) idømt dagbøder, eftersom T havde skaffet sig adgang til ekskærestens Facebook-konto, og lavet ændringer i profilopsætningen. T blev derfor fundet skyldig i STRFL § 263, stk. 2, ikke fordi T havde anvendt hacking programmer til at begå handlingen, men idet T havde udnyttet viden om

[42] Jf. Trzaskowski, Jan: Internetretten, side 614
[43] Jf. Trzaskowski, Jan: Internetretten, side 617ff
[44] Jf. Slade, Robert: Cybersercurity lessons from COVID-19, side 89f
[45] Jf. Danmarks Statistik: Halvdelen har oplevet it-sikkerhedsproblemer

adgangskoden og dermed skaffet sig en uberettiget adgang til kontoen. En adgang, der efter omstændighederne synes ham unddraget.
Af den grund udledes, at den kriminaliserede handling helt konkret er at tilgå og uberettiget skaffe sig adgang til andens data eller datasystem, uanset om det er ved hjælp af hackerværktøj. Et kendskab til en adgangskode eller det at knække en adgangskode giver ikke hackeren en berettiget adgang, hvilket indrammer kriminalisering, som beskytter de store datamængder, der kun er beskyttet af password på sociale medier. Det er op til en konkret fortolkning af hvert enkelt tilfælde for at udlede graden af offentlighed, tilgængelighed og herunder en persons berettigelse til den pågældende handling, idet en kortvarig tilgang til identitetsoplysninger ikke forudsætter en berettiget adgang til at benytte dem i andre handlinger, Jf. U.2020.4284. Der er tale om en afvejning af hensyn i forhold til en legitim adgang, og i praksis vil der i så fald være tale om et interessefællesskab, herved ægteskab, forretningsforhold, ansættelsesforhold mm., hvorved der foreligger en gyldig fuldmagt, der kan legitimere og berettige den pågældende handling, hvilket ikke var tilfældet i denne sag, hvorfor T blev dømt efter hackingbestemmelsen.

Det følger endvidere af U.2018.933, hvor landsretten henfører det strafbare forhold under hacking bestemmelsen, jf. STRFL § 263, stk. 2, jf. til dels § 21, idet tiltalte ved at installere keyloggere havde haft henblik på at kopiere og gennem personoplysninger angående brugernavn og NemID, og dermed uberettiget skaffet eller forsøgt skaffe sig adgang til en andens oplysninger gennem et informationssystem. I dette tilfælde var der tale om identitetstyveri af 8 identiteter, hvorved der var konstateret installation af 7 keyloggere og forsøgt installation af yderlig 47 keyloggere. Et samlet udbytte på 1,8 mio. kr., hvorfor der var tale om nøje planlagt kriminalitet af professionel karakter og derfor en højere straframme på 2 år og 6 måneder, grundet forbrydelsens omfang. Højesteret tiltrådte endvidere i U.2018.1787 at hackerangreb kan bedømmes samlet, og dermed straffe i sammenstød. I denne sag var der tale om særligt skærpende omstændigheder efter § 263 stk. 3, eftersom tiltalte, som tidligere ansat, havde begået hackerangreb i 78 tilfælde for en værdi på 740.000 kr., hvormed T ifaldt en straf på 3 år og 6 måneder grundet omstændighedernes korte tidshorisont og forbrydelsens omfang, som skærpende omstændighed.

Af ovenstående sager kan henføres, at hacking ofte bliver brugt som indgangsvinkel til at begå andre forbrydelser, hvilket også blev statueret i U.2021.1166 hvor tiltale gennem hacking havde skaffet sig adgang til forurettedes computer, hvorfra han senere kunne bedrage dem i online pokerspil, se nærmere afsnit 3.3.2. Hackingbestemmelsen bliver derfor ofte brugt til at straffe i sammenstød med andre delikter, hvorfor denne strafbestemmelse vil være gennemgående i gennem kandidatspecialet, idet hacking forbrydelserne tager afsæt i senere kriminelle handlinger også i forhold til identitetstyveri, som nævnt i U.2018.933.

Hacking er underlagt en betinget offentlig påtale, hvilket vil sige, at forurettede, som offer, skal anmelde forholdet til politiet for at der kan igangsættes en straffesag, eller tilkendegive at man ønsker forholdet strafforfulgt. Med andre ord, er det den forurettede, der er under strafbestemmelsen, er undergivet privat påtale og dermed den, der tilkommer påtaleretten, idet den forurettede person er beskyttelsesobjektet for strafbestemmelsen, jf. STRFL § 275 om privat påtale.
Bødestraffen for overtrædelse af STRFL § 263 er tredoblet, efter lovændring L 2018 1719, som bygger på betænkning nr. 1563 om freds- og ærekrænkelser, hvor formålet er at styrke det strafferetlige værn mod krænkelser af privatlivets fred. En hacker kan således ifalde bøde eller fængsel i 1 år og 6 måneder for at tilgå identitetsoplysninger, såvel som fængsel straf i op til 6 år for systematisk og organiseret kriminalitet. Yderlig er § 263 a indsat i straffeloven, og kriminaliserer den, der sælger og udbreder data. En handling, hvor selve adgangen til identitetsoplysninger udbredes. Hvorimod STRFL § 263 stk. 2 værner om krænkelser af privatlivet, og kriminaliserer det at skabe mulighed for at krænke en andens privatliv. STRFL § 263 a, er indsat for at kriminalisere muligheden for at skaffe sig adgang, hvorved der skal være forsæt til at sælge for at § 263 a finder anvendelse, hvorimod der ikke kræves yderligt forsæt til en senere brug af password.

Det udledes derfor af ovenstående, at strafbestemmelsen rummer en beskyttelse af privatlivets fred, og dermed informationer, der kan forventes unddraget og vedstå privat. En *'uberettiget'* handling angiver, at bestemmelsen rummer bredt, hvorfor det er op til et konkret skøn at bedømme, om handlingerne er legitime eller efter ordlyden omfattes af bestemmelsen. Redskaberne brugt er ikke i sig selv strafbart, da oplysningerne kan være frit tilgængelig, og identitetstyven har dermed

ikke skulle begå en strafbar handling for at tilgå oplysningerne. Dog bemærkes, at viden omkring adgang eller password ikke frit kan udnyttes, hvilket blev statueret i U.2017.247V, hvormed det strafbare element efter hacking bestemmelsen er at tilgå en andens data uden reelt samtykke, hvorfor det endvidere er underforstået, om der er opnået kendskab til oplysningerne, idet selve adgangen kriminaliseres.

Såfremt identitetsoplysninger er offentlig tilgængelig information om en identitet, så er det dermed ikke *adgangen til oplysninger der er strafbart, men nærmere den efterfølgende handling, der er strafbelagt*[46]*,* se nærmere afsnit 3.3.1 og 3.3.2 om dokumentfalsk og bedrageri.

Alt i alt rummer STRFL § 263 en bred formulering, og da der ikke foreligger særlig stor retspraksis på området, efterlades en gråzone til fortolkning af forholdene i forhold til identitetstyveri. Strafbestemmelsen kan benyttes til at kriminalisere tilgangen til identitetsoplysninger. Fuldbyrdelse sker øjeblikkelig, idet der er forsøgt adgang, herved uden forudsætning til om der opnås kendskab til indholdet. Formålet med adgangen kan have betydning for strafudmålingen, og være formildende eller skærpende omstændighed.

3.2.2 Tyveri, jf. straffelovens § 276

Tyveribestemmelsen i STRFL § 276 rummer en borttagelse, der kan indrammes under første led af begrebsdefinitionen, idet tyven kan straffes for *uden samtykke fra besidderen at borttage en fremmed rørlig ting for at skaffe sig eller andre uberettiget vinding ved dens tilegnelse*. Strafbestemmelsen beskriver borttagelse af en fremmed rørlig genstand, hovedsageligt fysiske objekter af en økonomisk værdi. Tyveri indgår derfor som en berigelsesforbrydelse, nugældende formueforbrydelser i straffelovens kapitel 28, med modsatrettede hensyn, hvorved den ene side udgør vinding forud sat et tab på den anden side, som en uberettiget formueforskydelse[47]. Fuldbyrdelse sker øjeblikkelig ved borttagelse, hvorfor dette gælder som fuldbyrdelsesmoment, og identitetstyven skal da have forsæt til vinding gennem borttagelse, heraf et berigelsesforsæt. Endvidere indeholder STRFL. § 276 et subjektiv krav om handling, her at *skaffe sig uberettiget vinding* med forsætlig virkning, og dermed rummer den et tilegnelsesforsæt[48].

[46] Jf. Trzaskowski, Jan: Internetretten, side 612
[47] Jf. Waaben, Knud: Strafferettens specielle del, side 111
[48] Jf. Karnov: Note 1592 af LBKG 2020-11-17 nr. 1650 Straffeloven

Sammenholdes tyveribestemmelsen med identitetstyveri, kan det skabe forvirring om et individs identitet kan være genstand for en sådanne borttagelse af en fremmed *rørlig ting,* og stille supplerende spørgsmål ved om identiteten har en reel materiel værdi[49].

Borttagelsen stiller først krav om en *fremmed* genstand, hvilket naturligt er opfyldt ved identitetstyveri, idet identitetsoplysningerne vedrører den anden person, denne varetægt og derfor vil dette ikke yderlig analyseres. Mere interessant er sondring om en identitet er udtryk for en materiel genstand, og en genstand som kan forflyttes eller fratages. Her må det lægges til grund, at dokumenterne, nærmere identitetsoplysninger kan stjæles, så længe de er tilknyttet et fysisk objekt[50], og da tyveri kriminaliserer selve borttagelsen, stilles der ikke selvstændige krav til betydning om tingen, og at denne skal være rørlig[51], jf. U.1940.113 Ø. I denne sammenhæng må en ejendomsret indfortolkes, her retten til at eje sin egen identitet, da ting, der ikke er undergivet en ejendomsret, ikke kan stjæles. Tyveri omhandler derfor en tilegnelse og derved en borttagelse, som er formueforskydende.

Foruden den krænkelse der sker af ejendomsretten, nærmere retten til at råde over ens identitet, så at sige, så omhandler tyveri også et indgreb i, hvad personen besidder og dermed dennes varetægtsforhold. Sondringen om identitetsoplysningerne er i individets eller gerningsmandens varetægt, nærmere hackerens varetægt, er ikke en vanskelig vurdering. Varetægtsforholdet må alt andet lige følge, hvem der har de pågældende data i hænde, hvorfor varetægtsforholdet ved borttagelsen forflyttes. Her er det vigtigt at bemærke, at der i relation til tyveri skal være forsæt til varetægtsforholdet. Hvorfor hackeren skal have forstået de omstændigheder, som statuerer denne varetægt, og en *vildfarelse af begrebet er en egentlig retsvildfarelse*[52]. Det lægges derfor til grund, at identitetsoplysninger er underforstået genstand for *fremmed rørlig ting*, da oplysninger kan formueforskydes, og den anvendte fremgangsmåde indgår derfor under tilegnelse samt borttagelse af et fysisk objekt[53]. Idet identitetstyveri ofte tager afsæt i økonomisk vinding, statueres her et berigelsesforsæt, samt forsæt til tilegnelse.

[49] Jf. Waaben, Knud: Strafferettens specielle del, side 119f
[50] Jf. Toftegaard Nielsen, Gorm: Kommenteret straffelov, side 588
[51] Jf. Betænkning nr. 1032 af 1985 om datakriminalitet, specielle bemærkninger § 276, afsnit 3.2
[52] Jf. Waaben, Knud: Strafferettens specielle del, side 126
[53] Jf. Waaben, Knud: Strafferettens specielle del, side 119

Endvidere støttes det af bestemmelsen at gerningsmanden, her identitetstyven skal have handlet med vindingsforsæt, hvilket subjektivt stiller krav om en økonomisk værdi af genstanden. STRFL § 276 rummer ikke et udtrykkelig krav herom, men når dette sammenholdes med kravet om forudsat tab ved den anden part, kan vi udlede, at den omsættelig vare må have en sådan værd. Såfremt det borttagne er af affektionsværdi, omhandles det ikke af strafbestemmelsen i STRFL § 276, og i så fald skal dette forhold bedømmes for unddragelse i STRFL § 263, nr. 1.

Det følger, at den økonomiske værdi skal have en almindelig bytteværdi, hvorfor *tilegnelse af identitetspapirer som regel ikke kunne straffes efter tyveri, selv om formålet har været at opnå en uberettiget økonomisk fordel*[54], idet oplysninger ikke har en almenkendt bytteværdi. Forholdet kan undtagelsesvis henføres under bestemmelsen, hvis den videre brug forudsætter et nyt strafbart forhold[55]. Hvorfor identitetstyveri må kunne sammenholdes med tilegnelse af checkblanketter, som ved borttagelse ikke bevirker noget tab, men ved en senere uretmæssig brug kan straffes efter dokumentfalsk samt bedrageri. I den henseende kan det virke mere konkret kun at dømme for det beviste misbrug, dog må det på den anden side styrke det strafferetlige værn ved at kriminalisere en sådan handling ved borttagelse, der ofte har forsæt til vindingen gennem senere kriminel handling.

Ser vi nærmere på retspraksis, så må vi alt andet lige udlede, at identitetsoplysninger som de pågældende effekter, har en omsætningsværdi på det illegale marked, hvorfor det indgår i strafbestemmelsen af STRFL § 276, jf. U 1984.894 Ø. I denne sag blev tilegnelse af narkotika henført under tyveribestemmelsen til trods for den manglende lovlige omsætningsværdi, og dermed indrammer den strafbestemmelsen til også at omhandle effekter, der på det illegale marked har en omsætningsværdi. Det må efter omstændighederne alt andet lige være tilfældet for identitetstyveri, hvormed selve unddragelsen kriminaliseres, idet datamateriale om personen fratages med henblik på senere økonomisk vinding. Hvorfor der kan udledes, at identitetsoplysningerne har en omsættelig værdi, da hackeren kan sælge oplysningerne på det illegale marked eller benytte dem ved senere forbrydelser. Derved kan hackeren råde over identitetsoplysningerne[56], og da selve krænkelsen i strafbestemmelsen vedrører selve

[54] Jf. Toftegaard Nielsen, Gorm: Kommenteret straffelov, side 590
[55] Jf. Waaben, Knud: Strafferettens specielle del, side 120
[56] jf. Karnov: Note 1596 samt 1598 af LBKG 20-11-17 nr. 1650

varetægtsforholdet, er det en del af gerningsindholdet i strafbestemmelsen. Hvormed det af ovenstående antages, at identitetstyven ved fratagelse af identitetsoplysninger ofte har et subjektivt forsæt til alle led i gerningsindholdet på borttagelsestidspunktet[57] med henblik på en økonomisk vinding.

Yderlig kan der opstå forvirring omkring borttagelse i forhold til gerningsindholdet, idet der stilles krav om *flytning af genstanden*, her en flytning af identiteten, hvorfor der efter omstændighederne at tolke må forstås en flytning af identitetsoplysninger. I nogle tilfælde skal der ikke meget til at denne borttagelse sker. I den fysiske verden ville en tyv normalt kun skulle bevæge sig meget få meter med genstand eller have passeret kassen for, at der statueres et strafansvar. Dog må der ved identitetstyveri være tale om en øjeblikkelig fratagelse, og dermed når en aktiv handling er forsøgt. Idet, fuldbyrdelsesøjeblikket indtræder, når der aktivt tages handling, nærmere forstået når oplysninger om identiteten forsøges borttaget ved en online aktiv handling som hacking.
For at ifalde straf forudsætter handlingen forsæt, og handlingen må ikke være udslag af distraktion eller fejltagelse[58], hvilket kan være den omstændighed, at tyven ved forvirring kommer til at flytte eller medtage en genstand. Set i lyset af identitetstyveri vil borttagelsen af oplysninger kunne forekomme online og offline. Idet kandidatspecialet vedrører de online handlinger, vil det sjældent forekomme, at en tyv i forvirring borttager oplysninger om en anden persons identitetsoplysninger uden videre forsæt til handling. Ofte tager en sådan handling aktivt udgangspunkt i et berigelsesforsæt og dermed også et tilegnelsesforsæt, da gerningsmanden gennem aktive handlinger forsøger at få oplysningerne i hænde.

Af ovenstående udledes, at der som udgangspunkt, efter strafbestemmelsen, gælder en forudsætning om fysisk borttagelse af et objekt, hvilket kan skabe problemer i forhold til borttagelse af identitetsoplysninger. Dog kriminaliseres selve handlingen, herunder flytning af de pågældende oplysninger. Og så længe oplysningerne, som ved identitetstyveri, knytter sig til den enkeltes identitet, som fysisk objekt, kan identitetstyven efter STRFL § 276 straffes, medmindre der er tale om en distraktion eller fejltagelse ved tilkomsten af identitetsoplysningerne. Endvidere er det vigtigt

[57] Jf. Toftegaard Nielsen, Gorm: Kommenteret straffelov, side 597
[58] Jf. Waaben, Knud: Strafferettens specielle del, side 118

at bemærke, at § 276 ved *skaffe sig eller anden uberettiget vinding* behøver forsæt til berigelse ikke være et direkte berigelsesforsæt, da medvirkende, der ikke har berigelse for øje, alene overvejende skal finde det sandsynligt, at det er gennem handlingerne og selve tilegnelsen er til berigelse[59] for at ifalde straf. Identitetstyven kan således efter STRFL § 276 ifalde bøde eller fængselstraf i 1 år og 6 måneder, og for grove tilfælde op til 6 år, jf. STRFL § 285.

Normalvis kan der ved tyveri være tale om, at forurettede handler i nødværge efter STRFL § 13, hvorved forurettede forsøger at beskytte sine ejendele. Her gælder, at man normalt ville kunne løbe efter en tyv for at fratage det stjålne efter en umiddelbar reaktion i den overhængende handling. Såfremt der ikke længere er et overværende angreb, vil der være tale om selvtægt, hvilket ikke fritages for ansvar. I en digital kontekst vil der være tale om at beskytte ens data og identitet på samme måde som at beskytte fysiske genstande. For at beskytte disse objekter online, vil det kræve et modangreb, herunder hacking, for enten at afværge en borttagelse eller for at slette de stjålne oplysninger, med henblik på at tilkomme personoplysningerne og dermed råde over sin egen identitet.
Problematikken opstår, idet der normalt er tale om en reaktion i et overværende angreb, hvorimod der ved hacking og tyveri af identitetsoplysninger ofte er tale om afsluttede angreb. Tidshorisonten er svær at definere, og afhænger af en konkret fortolkning af angrebet.
Cyberangrebet er ikke afsluttet, hvis malware eller andre typer hackerværktøj er installeret på computeren, dog vil omstændighederne være en anden ved phishingangreb. Her har forurettede modtaget mail, hvor pågældende er manipuleret til at begå en handling, herunder bedraget til at oplyse de personidentificerbare oplysninger, hvorfor det ikke vil give mening at løbe efter tyven. Forholdene bør i den kontekst anmeldes, og strafforfølges af politiet gennem en retslig håndhævelse[60], da et modangreb sandsynligt vil statuere selvtægt i form af hacking. For at beskytte og værne sig mod disse angreb bør man tænke i andre baner. Det kunne være en såkaldt honeypot, hvor man laver et falsk offer for hackerne. Det vigtigste element i denne sondring er, at man juridisk set forbliver på sin egen banehalvdel, og her kun eksponerer de angreb, der tilkommer en for at beskytte sine data, hvilket i strafferetlige henseende ikke vil aktualisere et strafansvar, idet man

[59] Jf. Waaben, Knud: Strafferettens specielle del, side 128
[60] Jf. Waaben, Knud: Strafferettens specielle del, side 140

hermed registrerer og anmelder de forsøgte hacking angreb. Konkret er det op til en vurdering af domstolene, om en sådan forsvarsafværgeinstallation er lovlig, da der ikke er tale om en nødværgesituation, idet man installerer foranstaltningen, når der ikke er nogen igangværende angreb at forebygge mod. Hvorfor det fra ovenstående må udledes, at nødværge i en digital kontekst er vanskelig, da manglende fastlæggelse af retspraksis mangler.

I takt med en stigende udvikling af teknologien og med sociale mediers tilkomst er begrebet "offentlige rum" vokset, og dermed også behov for regulering af området. Af ovenstående analyse udledes, at den primære fredskrænkelse er brud på den daværende brevhemmelighed, og den sekundære handling er det, at videre udnytte de identitetsoplysninger, som er skaffet ved privatlivskrænkelse.
Identitetstyveri antages på baggrund af ovenstående antagelse at have en sådan omsættelig værdi, at der ved borttagelse statueres et berigelsesforsæt, såfremt hensigten med tilegnelsen er led i senere kriminel handling, som i dette kandidatspeciale rummer formueforbrydelser, jf. afsnit 3.3.
Endvidere rummer bestemmelsen også et tilegnelsesforsæt, som er grundlæggende for, at der kan statueres identitetstyveri. Det er dermed ikke kun tilegnelsen, som er kriminaliseret, men hackere kan ifalde strafansvar efter anvendelse af de identitetsoplysninger, som sekundær handling.
Da kandidatspecialet rummer begge begrebsdefinitioner, og ikke er afgrænset til at omhandle tilegnelsen af identitetsoplysninger, vil de efterfølgende afsnit omhandle selve anvendelsen af identitetsoplysningerne og nærmere selve identitetsmisbruget.

3.3 Misbrug af identitetsoplysninger:

Begrebsdefinitionen af identitetstyveri vedrører i andet led de efterfølgende handlinger og selve brugen af identitetsoplysninger og det nærliggende identitetsmisbrug i sin helhed. Identitetsmisbrug omhandler handlinger, hvor de personfølsomme identitetsoplysninger indgår i andre kriminelle handlinger. Der kan være tale om forbrydelser som dokumentfalsk og bedrageri, hvorfor følgende afsnit vil analysere, hvordan forholder strafferammen sig i forhold til identitetstyveriet. De delikter, vi ser nærmere på, vil være forbrydelser angående bevismidler, her dokumentfalsk, jf. STRFL § 171 og bedrageri i § 279.

3.3.1 Dokumentfalsk, jf. straffelovens § 171

STRFL § 171 er et delikt om dokumentfalsk under straffelovens kapitel 19 angående forbrydelser om bevismidler. Strafbestemmelsen rummer den, der gør brug af et dokument til at skuffe i retsforhold. I § 171, stk. 2 defineres, hvad der forstås med et dokument, nærmere *en skriftlig betegnelse med den af udstederen forsynet tilkendegivelse, der fremtræder til at tjene som bevis eller bliver benyttet som bevis for en rettighed*[61]. Det er her særligt vigtigt at forholde sig til det krav, at dataoplysninger også skal være en skriftlig tilkendegivelse, hvorfor datalagret oplysninger ikke udgør en sådan skrift, jf. Straffelovrådets opfattelse. De anser det nærmere som middel til at frembringe en senere skriftlig tilkendegivelse, som senere får bevismæssig betydning. Hvorfor ændringer i data kan være et led i at fremkalde et skriftligt dokument, og tjener derfor som forsøg på dokumentfalsk.
Strafbestemmelsen kriminaliserer den, der *gør brug* af et *falsk dokument med hensigt at skuffe i retsforhold*. I strafbestemmelsen er stk. 2 videre indsat for at omfatte elektroniske tilkendegivelser, der fremtræder og tjener som bevis, hvilket omfatter e-mails, sms og andre opslag på sociale medier og hjemmesider, forudsat indholdet af stk. 2 er opfyldt[62].
Endvidere rummer stk. 3 i første led *eftergørelse*, her forstås et dokument, der i form og indhold er opdigtet[63], samt andet led *forfalskning*, her særligt dokumenter, der ved udstedelse er falsk og dermed ikke identisk med den faktiske udsteder[64].

Strafbestemmelsen omtaler hensigtsdokumenter skabt til formål at tjene som bevis, hvorimod lejlighedsdokumenter ikke er skabt til formål at tjene som bevis, men i en konkret situation kan bruges til det. Ifølge Lovændring i 2004[65] medførte det, at STRFL § 171 nu alene rummer hensigtsdokumenter.

I gerningsindholdet fremgår ordet *falsk*, hvilket efter ordlyden har en bred definition. Begrebet rummer to variationer, derved et dokument, der ikke stammer fra den pågældende udgiver, samt dokumenter, der stammer fra den pågældende, dog med ændrede oplysninger. Eksempel på første

[61] Jf. Betænkning nr. 1032 af 1985 om datakriminalitet, specielle bemærkninger til § 171 jf. afsnit 8.1
[62] Jf. Karnov: Note 1062 af LBKG 20-11-17 nr. 1650
[63] Jf. Waaben, Knud: Strafferettens specielle del, side 286
[64] Jf. Karnov: Note 1067 af LBKG 20-11-17 nr. 1650
[65] Jf. L 2004-05-19 nr. 352 Ændring af straffeloven

variation kan være et forfalsket pas, og anden variation kan rumme et oprindeligt udstedt pas, hvor der er ændret i oplysninger såsom billedet. STRFL § 171 rummer begge typer dokumenter, og stiller dermed ikke nogen krav eller forudsætning for, at kun fuldstændig eftergjort dokumenter er omfattet. Hvormed det ikke er afgørende, om den ene af betegnelserne benyttes, men nærmere om betingelserne i stk. 3 er opfyldt.

Tilsvarende betyder det, at sondringen ikke konkret omhandler om det fulde navn er benyttet, men nærmere om pågældende gerningsmand har haft til hensigt at anvende en betegnelse med forsæt til at vildlede. Af denne sondring kan udledes, at selve tilkendegivelsen skal hidrøre fra personen, og sondringen nærmere angår det viljemæssige til at indestå for den.

Sammenholder man ovenstående sondring med eksempler på dokumentfalsk, kan det forekomme, at en underskrift er påført af en anden senere. Dette udgør ikke i sig selv, at dokumentet bliver falsk. I forhold til digitale dokumenter gælder det samme, at udstederen skal fremgå af selve dokumentet[66], og sagt på en anden måde, så består et ægte dokument i at hidrøre fra udstederen selv, og det er ikke tilfældet, hvis der foreligger misbrug af bemyndigelse eller alternativt, hvis der tilføjes noget til dokumentet, kan der nærliggende være tale om bedrageri, jf. STRFL § 279, særligt hvis der handles med berigelsesforsæt.

Strafbestemmelsen i STRFL § 171 forudsætter derfor, at dokumentet skal være overgivet eller forevist som ægte[67]. Bestemmelsen har derfor et fremrykket fuldbyrdelsesmoment, hvilket vil sige, at gerningsmandens forsæt alene skal række til at ville skuffe i retsforhold. Dette forudsætter altså ikke, at handlingen er fuldbyrdet eller, at der konkret er lidt et tab, men statuerer alene ansvar ved at hackeren forsøger at skuffe i retsforhold, og udøver handlingen og dermed fremlægger identitetsoplysningerne med forsæt til at skuffe i det pågældende retsforhold. I elektronisk kontekst, vil et dokument være leveret, så snart det er tilsendt og tilgængeligt i modtagerens indbakke. Hvorfor en frasorteret mail i spamfilter ikke er tilgængelig.

Det udledes derfor, at deliktet har fremrykket fuldbyrdelsesmoment, hvilket medfører, at når man har fremført deliktet, så behøver man ikke tilgå en sondring om frivillig tilbagetræden, jf. STRFL § 22, da handlingen er fuldført og dermed strafpålagt. Med andre ord betyder det, at der er et

[66] Jf. Betænkning nr. 1417 af 2002 om it-kriminalitet, side 105

[67] Jf. Waaben, Knud: Strafferettens specielle del, side 290.

subjektivt overskud, og dermed at hackerens forsæt skal række til, at der skuffes i retsforholdet med den anden part, som dermed lider et tab. En vigtig sondring er, at hvis modparten, her modtageren af dokumentet er bekendt med at dokumentet er falsk, så kan gerningsmanden ikke skuffe i retsforhold, og gerningsindholdet er dermed ikke opfyldt, hvorfor gerningsmanden ikke kan ifalde straf. Endvidere stilles der ikke krav til sammenhæng mellem dokumentet og det formål, som ønskes vildledt. Hvorfor der i forhold til identitetstyveri ikke behøver være en nærliggende sammenhæng i forhold til det ønskede formål, som tilsigtes ved brug af falske dokumenter, herunder pasdokumenter eller andre identitetsoplysninger. Det er alene viljen, og nærliggende forsøget på at skuffe i et retsforhold, som efter strafbestemmelsen er strafbelagt.

Endvidere kan omstændighederne, som at identitetsoplysningerne kommer den anden part i hænde, spille en afgørende rolle for de efterfølgende forpligtigelser. I U.2019.1197 blev A, der havde udleveret sine personlige oplysninger til tredjemand, aftaleretlig forpligtet af et digitalt gældsbrev og derved lån, som B havde optaget. A havde anført, at oplysningerne var blevet givet som udslag af tvang, hvilket, såfremt der er tale om mekanisk tvang, gør dokumentet falsk[68]. Højesteret anlagde, at en aftaleretlig forpligtigelse er op til en konkret sondring af omstændighederne, som i afsnit 3.5 omtalt besiddelse, kendskab til besiddelse samt efterfølgende handlinger for at minimere risici. Her byggede hæftelsen på en sådan grad af uagtsomhed, at A, som forurettede, ifaldt en aftaleretlige forpligtigelse.

Endvidere blev tiltalte i TfK2021.313 idømt 60 dages fængsel og dømt for dokumentfalsk og bedrageri efter STRFL §§ 171 og 279, dels § 21, ved svigagtig at have forsøgt at få bevilliget lån på 32.000 kr., ved at T havde udstedt falske lønsedler til bevillig af lån[69]. Af dommen udledes, at der sker overtrædelse af STRFL §§ 279 og 171, hvorfor der med denne dom kan statueres, at der kan straffes i sammenstød, hvilket ikke var gældende forud for lovændringen i 2004. Det er ikke kun i bedragerisager, hvor man udøver dokumentfalsk, og dermed ikke kun tilfælde med berigelsesforsæt, at man kan blive idømt. Dog omhandler dette kandidatspeciale hovedsageligt forbrydelser med økonomisk vinding gennem identitetstyveri, hvorfor der tages udgangspunkt i

[68] Jf. Knud Waaben: Strafferettens specielle del, side 289
[69] Jf. TfK2021.313

disse sager i forhold til udnyttelse af identitetsoplysninger ved senere kriminel handling. Da identitetsmisbruget ofte straffes i sammenstød med bedrageri, vil strafbestemmelsen nærmere nedenfor belyses, særligt i kontekst af de kendetegn, som statuerer straf. Straffen for dokumentfalsk vil derfor være bøde straf, samt fængsel i op til 6 år, jf. STRFL § 172, jf. § 171. Her er det vigtig at bemærke, at dokumentfalsk ikke længere absorberer ansvar for bedrageri[70].

Det udledes derfor, at strafbestemmelsen stiller krav om subjektivt forsæt i relation til egenskab ved dokumentet er falsk, og derfor gør brug af falsk dokument for at skuffe i et retsforhold, som har et fremrykket fuldbyrdelsesmoment. Dette kan forekomme ved identitetstyveri, og at nærliggende identitetsoplysninger misbruges, hvorfor gerningsmanden kan idømmes bødestraf eller fængsel på henholdsvis 2 år efter gerningsindholdet i § 171, og i særlig grove tilfælde en skærpet straframme på op til 6 år, jf. STRFL § 172.

3.3.2 Bedrageri, jf. straffelovens § 279 samt databedrageri § 279a

STRFL § 279 omhandler bedrageri, og er del af straffelovens kapitel 28 om formueforbrydelser. Strafbestemmelsen kriminaliserer det at *skaffe sig eller andre uberettiget vinding, ved retsstridigt at fremkalde, bestyrke eller udnytte en vildfarelse*, herunder bevirke en *handling eller undladelse,* der er *afgørende*, *hvorved nogen påføres et formuetab*. Bedrageribestemmelsen har på samme måde som tyveribestemmelsen et kendetegn ved, at der er forsæt til at bevirke en materiel formueforskydning, herunder vinding forudsat tilsvarende formuetab ved den forurettede, som medkontrahenten eller modpart. Hvorfor deliktet er omfattet af berigelsesforbrydelser, da der i strafbestemmelsen udtrykkeligt stilles krav om en uberettiget vinding, som formuetab[71]. Der kan endvidere forekomme sager, hvor der ikke konkret er sket en formueforrykkelse, men hvor ydelsen tilsvarende er økonomisk ækvivaleret den afgivne ydelse[72], og derfor omfattes af strafbestemmelsen.

Centralt for dette delikt er den *vildfarelse,* som karakteriserer selve strafbestemmelsen. Det er derfor det centrale ved bestemmelsen, at der er tale om en vildfarelse hos forurettede, og i omtalte

[70] Jf. Waaben, Knud: Strafferettens specielle del, side 292
[71] Jf. Waaben, Knud: Strafferettens specielle del, side 113
[72] Jf. Toftegaard Nielsen, Gorm: Kommenteret straffelov, side 581ff

emne, en vildfarelse hos individet eller modparten, som gerningsmanden har kontakt med. Vildfarelsen kan angå noget passeret, noget aktuelt, samt noget fremtidigt og vedrører ofte faktiske egenskaber. Herunder gælder, at der efter retspraksis også straffes for gerningsmandens subjektive forhold om opfyldelse af aftalen, idet bedrageri ofte opstår ved, at hensigten undlades eller forties, som derved er udtryk for de subjektive forhold[73].

Begrebet vildfarelse rummer også manglende forestilling om sammenhæng, herunder uvidenhed eller karakter heraf, samt bevisindhold, der ikke stemmer overens med virkeligheden. Det kan derfor udledes, at en faktisk vildfarelse kan angå mange omstændigheder, men efter ordlyden skal selve handlingen være bestemt til at fremkalde en handling eller undladelse, hvorfor der ved modparten skal foreligge en disposition, og dermed et valg i forhold til at aktualisere de motiverede grundlag[74]. Det er derfor op til en konkret vurdering af omstændigheder, for at vurdere om modparten har været genstand for en sådan vildfarelse.

Såfremt vildfarelsen er statueret, har det ikke konkret betydning, om gerningsmanden er kyndig eller ikke kyndig. Det er nærmere graden af selve uoverensstemmelsen mellem faktiske og de subjektive forhold hos modparten, som har betydning. Dertil stilles til dels krav om forsæt, og dermed at gerningsmanden *handler forsætligt* overfor en modpart med normalviden. For at handle forsætlig kræves handlingsforsæt, og det kan mangle såfremt gerningsmanden ikke har tillagt vildfarelsen samme betydning, herunder ikke tillagt oplysninger en betydning, som kan statuere en vildfarelse, og dermed mangler forsæt efter gerningsindholdet. Der kan være tale om, at parten alene har forsøgt at skjule eller undlade enkelte forhold, som at fremføre et urigtigt regnskab for at skjule sin økonomiske situation, jf. U 1937.1004 Ø, hvilket i pågældende sag ikke statuerede et strafansvar, idet hensigten og forsæt til vildfarelsen manglede.

Yderlig kan der statueres straffrihed, hvis modparten *bærer risikoen,* og dermed er bekendt med vildfarelsen, eller udtrykkelig har til hensigt alligevel at indgå retsforholdet under de pågældende omstændigheder. Hvorfor der kan udledes, at vildfarelsen skal have karakter af bestemmende indflydelse for, at der statueres en konkret vildfarelse, idet modparten under rette grundlag ikke ville have fortaget sin disposition. Såfremt gerningsmanden opnår adgang til data uden at vildlede en anden person, så er der ikke tale om bedrageri, idet der ikke foreligger en vildfarelse med

[73] Jf. Trzaskowski, Jan: Internetretten, side 594

[74] Jf. Waaben, Knud: Strafferettens specielle del, side 151

følgende dispositioner[75], hvorfor en række lignende bedrageriforhold kan falde uden for strafbestemmelsen i STRFL § 279, hvis der ikke er tale om en modpart, som er blevet vildledt til at handle eller undlade en disposition.

Ved nærmere fortolkning kan selve strafbestemmelsen opdeles i to, og dermed først den svigagtige handling gennem vildledelse, og dernæst de efterfølgende økonomiske konsekvenser, herunder økonomisk vinding og formuetab. Sammenholdes strafbestemmelsen med identitetstyveri og identitetsmisbrug, kan der være tale om at *fremkalde, bestyrke eller udnytte* en vildfarelse. Ofte vil der ved den svigagtige handling være tale om at *fremkalde* en vildfarelse, idet gerningsmanden eller hackeren råder over identitetsoplysninger, som antages at have bestemmende karakter og virkning i forhold til at vildlede modparten til aktivt at handle på deres vegne, efter pågældendes hensigt. Der kan i pågældende tilfælde være tale om handlinger så som at udstede lån, udlevere penge eller udlevere andre genstande, hvorved identitetsoplysningerne er fremlagt til at fremkalde en vildfarelse.
Såfremt der er tale om at *bestyrke* en vildfarelse, er der tale om en allerede bestående vildfarelse. Og hermed en vildfarelse, der kan underbygges ved fremlæggelse af eventuelle mundtlige eller skriftlige midler. Dernæst kan der være tale om at *udnytte* en foreliggende vildfarelse, herunder at indgå en handel hurtig eller tage imod en ydelse, hvor vilkårene bygger på et forkert grundlag, hvormed aftalegrundlaget er misvisende eller urigtig. Gerningsmanden kan dermed uforsætlig have fremkaldt en sådan vildfarelse, hvorfor det er vigtigt at sondre, om der af gerningsmanden kræves en positiv oplysningspligt. Det er vigtigt at bemærke, at strafbestemmelsen i STRFL § 279 med ordlyden *'udnytte'* angår passivitet som ansvarsgrundlag, dermed stilles ikke samme pligt til at fremkomme med positive oplysninger, og dermed rigtige oplysninger, som vil kunne undgå en vildledelse. Hvorfor der efter retspraksis statueres en vidtgående oplysningspligt. Det er derfor op til en fortolkning af selve retsstridigheden[76], om der er tale om en oplysningspligt eller acceptabel udnyttelse af omstændighederne, hvilket kan foreligge, hvis man under rette omstændigheder udnytter en fordelagtig markedsværdi ved anskaffelse af en genstand.

[75] Jf. Betænkning nr. 1032 af 1985 om datakriminalitet, specielle bemærkninger om § 279, jf. afsnit 6.5
[76] Jf. Waaben, Knud: Strafferettens specielle del, side 150

Anden del af strafbestemmelsen rummer fremkaldelse af en *uberettiget vinding*, og for at det kan rubriceres som en berigelsesforbrydelse, skal der foreligge berigelsesforsæt, hermed forsæt til en uberettiget økonomisk vinding ved deraf følgende tab for modparten. Et eksempel herpå kan være lånoptagelse eller udlevering af værdier, der på baggrund af vildledte identitetsoplysninger er indgået en aftale om.

Gerningsmanden kan ifalde straf med bøde eller fængsel op til 1 år og 6 måneder for overtrædelse af STRFL § 279, jf. § 285. Såfremt der er handlet forsætligt eller groft uagtsomt, og dispositionen bevirker til en vildfarelse, kan man efter STRFL § 300a pålægges straf i op til 8 år. STRFL § 300a svarer til § 279, den eneste forskel er at § 300a rummer en begrænsning, og dermed at tabet skal være *betydeligt*, hvorfor det ud fra forarbejder at tolke, må svare til en minimumsgrænse på 100.000 kr.[77]

Endvidere stilles der på samme måde som STRFL § 276 subjektivt krav for ansvar, herunder berigelseshensigt, nærmere kendt som *berigelsesforsæt*, hvilket kommer af ordlyden "*skaffe sig eller andre uberettiget vinding*". I dette delikt forudsættes alene, at gerningspersonen, her hackeren eller identitetstyven, har indset, at den pågældende handling og adfærd kan medføre risiko for tab, jf. U.1973.636 H (Ø). Tiltalte måtte indse at handlingen retsstridigt påførte den anden part en risiko for tab, hvorfor der kan udledes at strafbestemmelsen rummer forskellige grader af tilegnelsesforsæt.

Forsæt til handlingsbestemmelsen[78] kan dog være udelukket, som benævnt, hvis tiltalte alene har til hensigt at skjule sin egen situation, og dermed ikke har forsæt eller hensigt til at skuffe i retsforholdet, jf. U 1937.1004 Ø, idet tiltalte havde indtryk af, at de pågældende regnskabspapirer ikke var tillagt nogen særlig betydning. Det samme statueres i U.1997.772, hvor tiltalte manglede forsæt til bedrageri. Hvilket udleder, at der ikke altid er grundlag for at statuere det rette handlingsforsæt til at gennemføre gerningsindholdet.

Yderlig kan der statueres forsøg efter STRFL § 21 til dels § 279, til trods for modparten har været upåvirket af de vildledende oplysninger, idet forsøg straffer gerningsmanden, der har tillagt oplysningerne betydning med forsæt til at skuffe i retsforholdet. Desuden fungerer strafbestemmelsen om dokumentfalsk i § 171 som supplement til bedrageribestemmelsen, og kan

[77] Jf. Waaben, Knud: Strafferettens specielle del, side 160
[78] Jf. Waaben, Knud: Strafferettens specielle del, side 152

rumme et bedrageri[79], idet bedrageri ofte begås ved brug af et eller flere falske dokumenter[80], hvorfor flere sager ofte straffes i sammenstød. Og for at straffe for bedrageri må den pågældendes handling have fremkaldt, bestyrket eller udnyttet en vildfarelse, hvilket har fremkaldt en disposition hos modparten. I forhold til identitetstyveri tager bedrageri, i online tilfælde, ofte afsæt i hacking af identitetsoplysninger, hvorfor tiltalte I U.2021.1166 blev fundet skyldig i overtrædelse af § 263, stk. 3 samt § 279 stk. 2 samt forsøg herpå, jf. § 21. Idet T ved anvendelse af trojanske heste havde installeret programmer på forurettedes computer, og derigennem havde snydt dem i online pokerspil. Samlet blev 22,4 mio. kr. konfiskeret, og T ifaldt en straf på 3 års fængsel, idet T over en årrække havde begået hacking af skærpende karakter, samt bedrageri af særlig grov beskaffenhed. I denne sag blev hacking brugt som indgangsvinkel til at begå andre forbrydelser, og individets oplysninger blev misbrugt til bedrageri i de pågældende online pokerspil.

STRFL § 279 er en af de nyere delikter, da man tidligere havde den indstilling, at ofre selv måtte bære risiko for tab og den mulighed, at man kunne blive narret[81] af andre. Strafbestemmelsen er indsat primært for at regulere økonomiske forhold. I 1985 blev § 279a indsat i straffeloven, og er nu kendt som bestemmelsen om *databedrageri*. STRFL 279a minder om opbygningen og formulering af bestemmelsen i § 279, men indførelsen af § 279a har været resultatet af en ønsket kriminalisering af online bedrageri. Strafbestemmelsen kriminaliserer derfor en vildfarelse, der er opstået gennem en elektronisk databehandling[82], her mere konkret en automatiseret proces som eneste kontaktflade til forurettede modpart.

Første led i bestemmelsen beskriver det strafbare element at *ændre, tilføje eller slette oplysninger eller programmer*, samt andet led, den der *søger at påvirke resultatet af en sådan databehandling*. Handlinger hvorved der fortsat stilles krav til berigelsesforsæt. Tages udgangspunkt i CSC-sagen[83], omtalt i afsnit 3.2.1 angående hacking og hærværk af internetservere, så må det antages, at såfremt ændringerne var sket i berigelsesøjemed, og dermed med vinding for øje, ville sagen antageligvis være dømt efter STRFL § 279a, omhandlende databedrageri begået via en automatiseret proces. I stedet blev T idømt straf efter STRFL § 263, stk. 3, jf. stk. 2 samt § 291 stk. 2 om hærværk, idet

[79] Jf. Betænkning nr. 1032 af 1985 om datakriminalitet, specielle bemærkninger til § 279
[80] Jf. Waaben, Knud: Strafferettens specielle del, side 147
[81] Jf. Waaben, Knud: Strafferettens specielle del, side 146
[82] Jf. Waaben, Knud: Strafferettens specielle del, side 161
[83] Jf. U.2015.3615Ø

gerningsmanden tidligere var fundet skyldig i lignende tilfælde. Hvorfor der kan udledes, at nogle forhold fortsat vil henhøre under hærværks bestemmelsen i dansk ret, i det der foreligger en gråzone om "datahærværk". Det er i den henseende nærliggende kort at tale om den manglende kriminalisering af denne gråzone, da man under strafbestemmelsen i STRFL § 291 også skal indfortolke data under ordlyd "ting", hvilket er samme problemstilling benævnt under tyveribestemmelsen i afsnit 3.2.2. Dette kan give anledning til at påpege en manglende kriminalisering i dansk ret, idet den omtalte problemstilling selvstændig efter norsk ret kriminaliseres i strl. § 351 om skadeverk, med ordlyden "*for skadeverk straffen også den som uberettiget endrer, gjør tilføyelser til, ødelegger, sletter eller skjuler andres data* ", hvilket efter dansk ret antageligt ville omhandle datahærværk[84].

Fuldbyrdelsesmomentet ved § 279a ligger forud for § 279, idet det kan være en svær sondring, hvornår det konkrete forhold er fuldbyrdet til vinding. Tages udgangspunkt i første led, er det når der tages handling og her aktivt ændres noget. Tilsvarende vil momentet være, når man *søger at* påvirke, og dermed forsøger at gennemføre handlingen. Grundet fremrykket fuldbyrdelsesmoment vil mange sager, hvor begge delikter efter ordlyden kan benyttes, ønskværdigt straffes efter § 279a. Indsættelsen af STRFL § 279a belyser, hvor højt man efter dansk ret vægter STRFL § 1, og at der er den pågældende lovhjemmel. Idet STRFL § 279a er frigjort fra krav om, at der foreligger bevis for økonomisk tab, og i stedet for vildledelse nærmere omhandler indgreb i elektronisk databehandling. Derfor udledes det, at der i takt med den teknologiske udvikling, vil være behov for at regulere flere forhold, ligesom det er at regulere bedrageri lignende forhold i STRFL § 279a.

Bedrageren kan i sager som TfK2019.1411 ifalde straf for databedrageri med hensigt at begå identitetstyveri. Tiltalte 1 (herefter T1) og tiltalte 2 (herefter T2) fandtes skyldig i STRFL § 263, stk. 2 jf. stk. 3 til dels § 21, § 279 og § 279a, jf. § 286, stk. 2, jf. til dels § 21, da de systematisk og organiseret havde installeret keyloggere på biblioteker for at kopiere identitetsoplysninger om brugerne med henblik at begå databedrageri. T1 ifaldt en straf på 5 års fængsel, hvorimod T2 blev idømt 3 års fængsel for de nævnte forhold, som blev begået over en tidshorisont på henholdsvis 6 måneder og 2 måneder. Begge tiltalte var tidligere straffet for berigelseskriminalitet, og T1's ledende rolle, samt

[84] Jf. Lov 19 juni 2009 nr. 74, jf. § 351 om skadeverk

T2 handlinger, begået inden for prøvetiden, var medvirkende som strafskærpende omstændighed.

Som anført ovenfor starter identitetstyveri ofte først ved at gerningsmanden begår hacking efter STRFL § 263, for dernæst at begå anden kriminalitet. Hvis hackeren misbruger de personidentificerbare oplysningerne, kan handlingerne omfattes af bedrageribestemmelsen i STRFL § 279. Desuden kan der i sammenstød straffes for dokumentfalsk, som anført i U 2018.1787 hvor tiltalte blev fundet skyldig i bedrageri, databedrageri samt dokumentfalsk, efter STRFL § 263, stk. 3, samt §§ 279, 279a, § 171 og § 290 for hærværk. Retten fandt T skyldig i samlet 78 tilfælde at have bedraget for 740.000 kr., og derfor blev strafferammen udmålt under skærpende omstændigheder til 3 år og 6 måneder fængsel, idet forbrydelsernes omfang havde en systematisk og organiseret karakter. Endvidere fremgår af retspraksis, at tiltalte ved fremlæggelse af falske lønsedler havde forsøgt at få bevilliget lån på 32.000 kr. Tiltalte må efter omstændighederne at dømme have handlings- og berigelsesforsæt til at udføre dispositionerne, og derigennem forsøgt bedrageri gennem dokumentfalsk efter STRFL jf. § 172, jf. § 171, samt § 285, jf. § 279, jf. § 21, idet forurettede led risiko for tab[85].

Det kan af ovenstående udledes, at identitetstyveri alt efter fremgangsmåden, kan omfattes af strafbestemmelsen i § 279 samt § 279a, idet deliktet først som central del rummer moment af vildfarelse samt formuetab ved den konkrete handling eller undladelse, hvilket også kan ske gennem elektronisk databehandling. Forudsætning for, at der sker vildfarelse er, at denne har karakter af en bestemmende indflydelse, idet modparten, såfremt denne bekendt med rette vilkår, havde ageret anderledes og ikke uden lige tiltrådt samme vilkår. Desuden stilles krav til forsæt, herunder at skuffe i retsforholdet, hvorfor det er altafgørende at gerningsmanden har eller burde have indset modparten kunne lide tab, som følge.
Hvis handlingerne omhandler en uberettiget anvendelse af personoplysninger online, vil det antageligt blive behandlet under bedrageri og hacking bestemmelsen i henholdsvis i STRFL § 279, nærmere § 263, hvis tilegnelsen er sket elektronisk. Såfremt tilegnelsen er sket med henblik på at slette, ændre eller tilføje oplysninger, kan det strafbare forhold dels indgå i STRFL § 279a, som har et fremrykket fuldbyrdelsesmoment i forhold til § 279. Såfremt der er tale om fremlæggelse af falske

[85] Jf. TfK2021.313

dokumenter med henblik på en uberettiget vinding, vil gerningsmanden efter antagelse ved identitetstyveri ifalde straf efter STRFL § 171 dels § 279, samt § 276 eller § 263 alt efter, hvordan informationerne er kommet pågældende gerningsmand i hænde.

Idet strafferammerne for at ifalde straf efter identitetstyveri i ovenstående afsnit er belyst, vil følgende rumme en nærmere analyse af ofrene, herunder hvem der kan ifalde straf, og dernæst undersøge om forurettede, som offer for identitetstyveri, kan blive aftaleretligforpligtet af de kriminelle handlinger.

3.4 Forsøg og medvirken

Identitetstyveri rammer en bred definition, som ovenfor beskrevet, hvorfor de kriminelle handlinger alt efter fremgangsmåde kan straffes efter STRFL §§ 171, 263, 276 samt 279. Gerningsmændene kan have vidt forskellige forsæt til at begå handlingerne, hvorfor identitetstyven kan være alt fra private aktører til professionelle hackere. Det er dermed ikke alene private aktører, der kan ifalde straf. Man kan også blive strafferetlig ansvarlig, såfremt man gennem sit virke udnytter hverv og derved sin position, og bevirker at have påført en betydelig skade eller særlig risiko for identitetstyveri, hvorfor dette kort vil benævnes. En ansat blev i U.2016.2074 idømt 60 dages fængsel for uberettiget videregivelse af personlige oplysninger, herunder CPR. -nummer samt NemID-oplysninger, idet tiltalte *havde misbrugt sin stilling*. Retten fandt at tiltalte efter omstændighederne havde påført forurettede en sådan *skade eller særlig risiko* for skade, da videregivelse kunne udmunde i *identitetstyveri med økonomisk tab til følge*, hvorfor tiltalte blev idømt straf. Strafpålæggelsen i denne sag medvirker til et øget fokus på at indramme og kriminalisere de strafbare handlinger under identitetstyveri, da de kan have vidtgående konsekvenser, når først identitetsoplysningerne bliver misbrugt.

I ovenstående afsnit har vi analyseret rammerne for at idømmes straf efter de enkelte strafbestemmelser. Kendetegnet for mange af sagerne er, at der statueres ansvar til dels for forsøg og medvirken, dette beror på at gerningsindholdet ikke helt er realiseret, hvorfor der i STRFL §§ 21 og 23 er mulighed for at straffe for forsøg eller medvirken til den kriminelle handling. For at statuere ansvar og idømme straf for en kriminel handling, så er fuldbyrdelsestidspunktet relevant. Såfremt

man gennem hacking tilgår identitetsoplysninger, sker fuldbyrdelse øjeblikkeligt, og hvis der ikke opnås en sådan adgang, kan der i samme ombæring straffes for forsøg, jf. UfR 2002.1064 V samt U.2000.1450 Ø, hvorfor tiltalte i begge domme blev kendt skyldige i forsøg på hacking.

Efter STRFL § 21 er det muligt at straffe den, som alene forsøger eller har *forsøgt* at begå en strafbar handling, herunder "*handlinger, som sigter til at fremme eller bevirke udførslen af en forbrydelse, straffen når denne ikke fuldbyrdes, som forsøg"*. Hvorfor en overtrædelse, der dømmes efter forsøg, som udgangspunkt er den samme som ved fuldbyrdelse af handlingen[86], og vil derfor nærmere anføres "jf. pågældende paragraf, jf. § 21", som set i U.2018.993. I sagen blev tiltalte fundet skyldig i STRFL § 263, til dels § 21 for fremskaffelse og besiddelse af identitetsoplysninger, der gennem 8 keyloggere var realiseret. Yderlig havde T forsøgt på at installere 41 keyloggere for at skaffe yderligere identitetsoplysninger omkring NemID med henblik på at begå identitetstyveri og skaffe sig økonomisk vinding. I sagen blev forsøget på yderligere kriminalitet medregnet i den summerede straf, som tiltalte blev idømt. Det samme gør sig gældende i TfK2019.1411, hvor hackere på baggrund af at placere keyloggere på biblioteker havde til hensigt senere at begå identitetstyveri og databedrageri, idømt straf efter STRFL § 263, §21, § 279 og § 279a, jf. § 286, grundet omfang.

Vi kan af ovenstående konkludere, at man kan ifalde straf ved at begå og fuldbyrde den strafbare handling, men nærliggende også de som foretager handlinger, der kan udmunde i en begået forbrydelse, såfremt handling er forsøgt. Endvidere kan hackere efter STRFL § 23 ifalde straf for medvirken, herved straffes den der "*ved tilskyndelse, råd eller dåd har medvirket til gerning"*, blive straffet. Strafbestemmelsen i STRFL § 23 er generel, og det betyder, at der kan idømmes straf for medvirken i forhold til straffeloven og speciallovgivning. Såfremt den strafbare handling kræver forsæt, kræves dette også for at statuere medvirken, hvorfor der stilles krav om forsæt til at begå den efter ordlyden strafbare handling hos den medvirkende[87].

STRFL § 21 og 23 kan som nævnt anvendes i forlængelse af straffelovens speciallovgivning, idet det er strafbart at hjælpe en anden med at begå en forbrydelse, og hermed at foretage handlinger, som

[86] Jf. Trzaskowski, Jan: Internetretten, side 578
[87] Jf. Trzaskowski, Jan: Internetretten, side 580

udmunder i en overtrædelse. Hvorledes de enkelte handlinger skal subsumeres angår selve gerningsindholdet og mere konkret, hvordan identitetstyveri bliver realiseret, hvorfor der ofte idømmes straf i sammenstød for overtrædelse af straffelovens delikter.

3.5 Aftaleretlige forpligtigelser

Når strafansvaret er belyst, er en anden vigtig sondring i forhold til identitetstyveri, om forurettede, som individ, bliver ansvarlig for de pågældende handlinger, hvor identitetsoplysningerne navnlig er blevet misbrugt til at indgå aftaleretlige forpligtigelser, som følger. I 2021 oprettede B en række lån i A's navn, da B var kommet i besiddelse af hendes nøglekortoplysninger, og endvidere havde fået adgang til familiens tablet, hvor brugernavn og adgangskode var tilknyttet. B havde under handlingerne gjort alt for, at A ikke skulle opdage identitetsmisbruget, hvorfor man efter en samlet vurdering af omstændighederne fandt at A, som offer, ikke havde udvist en sådan grad af uagtsomhed og derfor ikke var aftaleretlig bundet[88]. Der er tale om, at der i dansk ret gælder en beskyttelse af individerne. Her, at man ikke aftaleretlige forpligtes, hvis en anden uberettiget i ens navn falsk eller ved ændring, nærmere forfalskning, benytter ens identitetsoplysninger. Idet det kan gøres gældende som ugyldighedsgrund mod en løftemodtager i god tro, hvorfor løftet kun binder den, som har afgivet oplysningerne eller den, som har rette fuldmagt til at afgive løftet. Undtagelse hertil er, hvis forurettede ikke forsøger at modvirke misbruget, og ved handling eller undladelse uagtsomhed tillader risiko for misbrug, kan denne ifalde en pågældende forpligtigelse.

Af retspraksis fremgår, at en konkret vurdering af hændelsesforløbet ligger til grund for om individerne hæfter og bliver aftaleretligt forpligtet, herunder hvilke omstændigheder tilegnelsen er sket, om der er kendskab til besiddelse af personidentificerbare oplysninger, samt hvad der er gjort for at minimere risici og forhindre misbrug, jf. U.2019.1192H samt U.2019.1197H.
I U.2019.1197H angik sagen, om der kunne ske tvangsfuldbyrdelse af de indgående forpligtigelser på baggrund af tredjemands misbrug af identitetsoplysninger. Forurettede havde i sagen udleveret sine oplysninger til tredjemand, som derefter, uden forurettedes kendskab og medvirken, havde optaget lån. Højesteret anfører, at det er op til en samlet vurdering af samlet hændelsesforløb,

[88] Jf. AFGR:2021-0226-4

herunder en konkret vurdering af "*hvilke omstændigheder tredjemand er kommet i besiddelse af indehaverens nøgle, 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*". Højesteret tilføjede, at forurettede havde udvist en sådan grad af uagtsomhed, at denne i forhold til de indgående forpligtigelser på aftaleretligt grundlag hæftede. Det udledes derfor, at det i hvert enkelt tilfælde er op til en konkret vurdering af hændelsesforløbet at vurdere omstændighederne, hvorpå identitetstyveriet er foretaget. I denne sag, fandt retten trods forurettede havde følt sig truet til at udlevere identitetsoplysninger, at være bundet af de indgående forpligtigelser, idet forurettede havde udvist en sådan grad af uagtsomhed[89].

Det følger af retspraksis, at man som udgangspunkt ved identitetsmisbrug ikke hæfter for de indgående forpligtigelser, dog kan et sådan misbrug være svært at definere, hvorfor man kan risikere at hæfte for misbrug af eksempelvis NemID-oplysninger, som set i U.2019.1197H. Undtagelsen til hovedreglen omfatter det scenarie, at forurettede har muliggjort misbruget, hvorfor forurettede i så fald hæfter for de indgående forpligtigelser og dertilhørende økonomiske tab. Forurettede kan efter omstændighederne have udleveret personoplysninger, og derved enten aktivt eller passivt gjort oplysningerne frit tilgængeligt. Forholdet vurderes ud fra det konkrete grundlag og de i sagen fremlagte omstændigheder. Det bør derfor afvejes, om der er tale om en sådan grad af uagtsomhed, hvormed offeret kan hæfte for de lån, der optages i deres navn[90].

Et eksempel på en sag, hvor forurettede A og B egenhændigt udleverede NemID-oplysninger til tredjemand, der udgav sig for at være fra politiet, som efterforskede et hackerangreb. Gerningsmanden havde dernæst optaget lån. I denne sag blev de tidligere U.2019.1192 samt U.2019.1197 gengivet i forhold til om individerne, som offer for identitetstyveri, aftaleretligt var forpligtiget af de af gerningsmandens indgående aftaler. A og B påstod, at de havde udleveret oplysningerne i god tro, men fogedretten fandt, at de havde handlet i en sådan grad af uansvarlighed. Sagen kæres og Landsretten fandt det betænkeligt at fremme en sag mod personer, der havde været udsat for identitetstyveri[91], idet lånet blev optaget uden medvirken og accept af A og B, samt de forhold at lånbeløbet var hævet samme dag, som det blev optaget, og uden senere at

[89] Jf. U.2019.1197H
[90] Jf. Teleankenævnet: Sag: 17-91 samt 17-212
[91] Jf. U.2020.3899

have medført nogen aktivitet på kontoen. Yderlig lægges til grund, at A undervejs forsøgte at minimere risici, og handlede ved at anmelde omstændighederne, så snart denne blev bekendt med et muligt misbrug. Landsretten fandt derfor, at det efter en samlet vurdering var betænkeligt at fremme sagen, og derfor nægtes fremme.

Sondringen af uagtsomhed kan henføres til, at det i nogle tilfælde kan være berettiget kortvarigt at udlevere sine identitetsoplysninger, herunder NemID og andre adgangskoder, som anført i U.2020.4284, hvor forurettede havde brug for hjælp til spærring af kort. At modparten efterfølgende svigagtig optager lån, og flytter individets konti, synes ikke at statuere en uagtsomhed ved identitetsofferet. Modsat følger det af sagen i U.2021.1268, at A havde udleveret sine personlige oplysninger til daværende kæreste, som senere havde optaget lån i forurettedes navn. Retten fandt, at forurettede ikke havde ført kontrol med, hvad oplysningerne blev brugt til, og derfor havde udvist en sådan grad af uagtsomhed, hvorfor A aftaleretligt var forpligtet af lånoptagelsen. Det kan derfor udledes, at man som offer for identitetstyveri har en forpligtigelse til at minimere risici. Såfremt man bliver bekendt med et mulig misbrug, er det vigtigt, at man minimerer omstændighederne, straks tager kontakt til de involverede parter og underretter omkring den pågældende mistanke. Endvidere kan individer for at undgå, at der optages lån eller køb i pågældendes navn, sætte et kreditvarsel på CPR-nummer, hvilket giver et signal om, at virksomheder samt banker skal være påpasselig, før de yder en sådan service[92].

Af ovenstående retspraksis konkluderes, at det er op til en konkret vurdering af omstændighederne, herunder særligt "*hvilke omstændigheder tredjemand er kommet i besiddelse af indehaverens* informationer *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*"[93], for at ifalde ansvar. Alt efter udfald kan forurettede ifalde en aftaleretligforpligtelse, hvis der er handlet med en sådan grad af uagtsomhed.

[92] Jf. Forbrug.dk: Forbrugere hæftede for misbrug af deres Nem-ID
[93] Jf. U.2019.1192 samt U.2019.1197

Kapitel 4

4.1 Kriminalisering af identitetstyveri

Af ovenstående analyse kan det konkluderes, at identitetstyveri er en udfordring i det strafferetlige værn. Problematikkens omfang kendes ikke konkret, idet der foreligger et større mørketal, grundet manglende registrering. Således er det kun sager, hvor anmelderen og sagsbehandlere egenhændigt anmelder og noterer, at der er tale om identitetstyveri, som fremgår af statistikkerne, hvilket alt andet lige må udledes at være en brøkdel af de tilfælde, som reelt sker. Dette kan skyldes den manglende fokus på denne kriminalitetsform, idet identitetstyveri ikke selvstændigt er kriminaliseret i dansk ret, hvilket muliggør en gråzone i det strafferetlige værn. Det fremgår endvidere af Justitsministeriet rapport[94], at trods indførelse af en mulig søgenøgle under identitetstyveri, at området stadig vil medføre usikkerhed om relevante sager opdateres korrekt. Hvorfor denne udtalelse kan medvirke til at understrege vigtigheden af en kriminalisering af identitetstyveri, særligt med henblik på at kunne følge og regulere retsområdet i forhold til digitale samfundets udvikling.

Identitetstyveri og identitetsmisbrug kan efter nærmere fortolkning af fremgangsmåde henføres og straffes under delikter som dokumentfalsk, hacking, tyveri og bedrageri, jf. kapitel 3. I analysen udledes, at der kan forekomme tilfælde, hvor det er svært at definere om der reelt er sket noget strafbart, idet det kan konkluderes, at det ikke i sig selv er ulovligt at sjæle en anden identitet. Som udgangspunkt gælder, at identitetstyveri ikke er strafbart, medmindre den strafbare handling vedrører andre delikter, idet gerningsindholdet skal matche med den pågældende strafbestemmelse, og dermed opfylde de konkrete strafbarhedsbetingelser for at ifalde straf. Endvidere er retspraksis på området minimal, hvorfor det konkret er op til domstolenes vurdering om pågældende tilfælde kan statuere et ansvar, til trods for de af identitetstyveri vidtgående konsekvenser, idet forurettede efterlades med psykiske og økonomiske konsekvenser.

Begrebet identitetstyveri har de seneste år været til debat, dog mangler der et politisk flertal for, at den særskilt kan blive kriminaliseret i straffeloven. I takt med området har fået mere og mere fokus,

[94] Jf. Retsudvalget spørgsmål 108-109 – Folketingsåret 2014-15: 2. samling

er der af flere omgange fremsat lovforslag om direkte kriminalisering af identitetstyveri og identitetsmisbrug, jf. Beslutningsforslag B 186 samt B 272.

Forud for disse beslutningsforslag, har der løbende været fremsat forslag til at bestyrke området, herunder i B 3[95] om straf for identitetstyveri og identitetssvindel, samt B 100[96] om sikring af personnummer med henblik på at bekæmpe identitetstyveri og identitetsmisbrug. Følgende afsnit vil kort bemærke nogle af de hovedpunkter, som i beslutningsforslaget fremføres i forhold til en ønsket kriminalisering.

4.1.1 Beslutningsforslag B 186 om særskilt straf for identitetstyveri og identitetsmisbrug

Det fremgår af B 186, fremsat 13. april 2016, som revideret genfremsættelse af B 3, at formålet med fremsættelse af dette forslag er at sætte fokus på de kriminelle handlinger, og kriminalisere identitetstyveri og identitetsmisbrug særskilt, så de to kriminalitetsformer *kan straffes med fængsel i op til 2 år*. Kriminalitetsformen forekommer hyppigere i takt med digitaliseringen, og skal derfor i højere grad prioriteres, mener Dansk Folkeparti. De udtaler endvidere, at ”*der er brug for en selvstændig kriminalisering, der medfører en selvstændig registrering, så udviklingen i denne kriminalitetsform kan følges nøje. Dette er afgørende for, at der kan sættes ind med de rette værktøjer og i det rette omfang*[97]”. Formålet er at fremsættelsen skal have en præventiv effekt, og dermed sende et signal om, at det er ulovligt at stjæle og svindle med andres identiteter. Hvorfor en kriminalisering medvirker, at identitetstyveri og identitetsmisbrug i højere grad skal prioriteres. Dette særligt, da Danmark i takt med internettets udbredelse og digitalisering i højere grad udleverer identitetsoplysninger på internettet, og derfor bliver mere sårbare i forhold til identitetstyveri.

Forslaget henviser til den norske kriminalisering af området, idet den norske strl. § 202 kriminaliserer den, der uberettiget sætter sig i besiddelse af en andens identitet, eller den, som optræder med denne identitet eller såfremt den er let at forveksle. Forslagsstillere henviser til at følge norsk praksis i forhold til identitetssvindel, og lade sig inspirere heraf, se nærmere afsnit 4.2.1.

[95] Jf. B 3 – 2011-12
[96] Jf. B 100 – 2012-13
[97] Jf. B 186 – 2015-16, jf. prioritering af området

4.1.2 Beslutningsforslag B 272 om kriminalisering af identitetstyveri og identitetsmisbrug

Det fremgår forud for fremførsel af B 272, at der er gennemført adskillige tiltag med henblik på sikring, afhjælpning og forebyggelse af identitetstyveri, herunder nedsat en tværministeriel arbejdsgruppe, som skal fremkomme med mulige løsninger til at regulere indholdet og ansvar, særligt af sociale medier, samt imødekomme andre initiativer til beskyttelse af området. B 272, er fremsat 9. marts 2021 af Socialistisk Folkeparti, som udtrykker følgende: "*I lyset af de seneste alvorlige sager om identitetstyveri og identitetsmisbrug mener forslagsstillerne, at der er et højaktuelt behov for snarest at få forhindret disse forbrydelser. Derfor pålægges regeringen i indeværende folketingssamling at fremsætte et lovforslag, der direkte kriminaliserer identitetstyveri og identitetsmisbrug*." Forslagsstillere mener, at identitetstyveri skal være strafbart med en særskilt paragraf i straffeloven, og herved kriminalisere identitetstyveri, også selvom der ikke er sket et efterfølgende identitetsmisbrug. Det strafbare forhold bør alene vedgå det forhold, at man udgiver sig for at være en anden. Formålet er at signalere en beskyttelse af ofrene for identitetstyveri og samtidig udtrykke, at det ikke er acceptabelt fra samfundets side.

En ny strafbestemmelse skal således have en præventiv effekt, idet der skabes et mindsket incitament hos gerningsmanden til at begå identitetstyveri. Hvorfor straframmen, skal afspejle at det ikke økonomisk kan betale sig.

4.1.3 Kriminalisering af identitetstyveri – ny § 264 e

Den 21. april 2021 er der yderlig fremsat et borgerforslag om kriminalisering af identitetstyveri, herunder forslag til en ny strafbestemmelse i STRFL § 264 e, der vil have følgende ordlyd:

" *Stk. 1. Den, der uberettiget anvender en andens billede, navn, personnummer eller andre lignende personoplysninger, på en måde der er egnet til at skabe forveksling med personen hos tredjemand, straffes med bøde eller fængsel indtil 6 måneder.*

Stk. 2. Sker overtrædelsen som led i en overtrædelse af straffelovens kap. 24 eller 28, kan straffen stige til fængsel indtil 1 år"[98].

[98] Jf. Borgerforslag.dk: Kriminalisering af identitetstyveri – ny § 264 e, i straffeloven

Lovforslaget fokuserer på at kriminalisere uberettiget identitetsmisbrug, idet der ofte er to ofre, den forurettede, som får identiteten misbrugt, samt den som identiteten misbruges overfor. Hvorfor forslaget ønsker at kriminalisere brugen af personoplysninger, herunder tilføje andre lignede personoplysninger, som er anvendt til at skabe forveksling hos modparten, med det formål at øge beskyttelsesrammen af hensyn til ofrene. Forslaget vil derfor frigøres fra at skulle henføre gerningsindholdet under andre delikter, idet det ikke er afgørende om fuldbyrdelse af gerningen er led i anden kriminel sammenhæng.
Stk. 2 må ud fra ordlyden fortolkes indsat, som et særligt skærpende moment, såfremt identitetsmisbrug bruges som led i anden kriminalitet i forhold til straffelovens kapitel 24 og 28 om henholdsvis seksualforbrydelser og formueforbrydelser.

Af forannævnte beslutnings- og lovforslag kan udledes, at der i det strafferetlige værn er enkelte huller i forhold til regulering af identitetstyveri i national ret, idet der er *usikkerhed om omfanget og selve behandling af sager, der anmeldes*[99], da området ikke direkte er kriminaliseret, og derfor kun indirekte straffes, hvor anden forbrydelse er begået. På baggrund heraf må der i dansk ret antages at mangle en klar regulering samt gerningskode til anmeldelse af sager omkring identitetstyveri, idet retspraksis på området efterlades til fortolkning.
Til trods for området de seneste år har fået større og større fokus, idet flere udsættes for identitetstyveri og identitetsmisbrug, mangler rammerne for identitetstyveri stadig at blive defineret, idet andre lande har kriminaliseret identitetskrænkelse selvstændigt i national ret. Hvorfor det kan give anledning til at se nærmere på grundlaget for vedtagelse af en særskilt strafferetlig regulering i henholdsvis norsk og svensk ret.

4.2 Komparativ analyse

I følgende afsnit vil retstilstanden i Danmark sammenholdes med den norske og svenske strafferetlige regulering af identitetstyveri, nærmere "*identitetskrenkelse"* samt "*olovlig identitetsanvändning*".

[99] Jf. B 186 – 2015-16

4.2.1 Lov 19 juni 2009, nr. 74 om "identitetskrenkelse" – Norsk straffelov

Norge har ifølge de tre nordiske lande, været foregangsland til at kriminalisere identitetstyveri under kapitel 21 om "Vern av informasjon og informasjonsutveksling", idet de i år 2005 indførte en ny strafbestemmelse, om "*identitetskrenkelse"*, som følger af strl. § 202:

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

a) oppnå en uberettiget vinning for seg eller en annen, eller

b) påføre en annen tap eller ulempe."

Med ovenstående strafbestemmelse kriminaliseres den, som krænker en identitet, herunder stilles særligt krav om forsæt til at opnå *uberettiget vinding*, eller det at *påføre en anden tab eller ulempe*. Såfremt det er overvejende sandsynligt, at handlingerne vil påføre nogen tab, vil dette også statuere et sådant ansvar, efter indholdet i § 202. Det er endvidere vigtigt at bemærke, at der efter norsk ret statueres ansvar, såfremt gerningsmanden opnår en fordel, og dermed stilles ikke et direkte krav til vindings- eller skadeshensigt, andet end en bagatelgrænse, og hermed at forholdet skal rumme en ulempe, der er højere end forurettes ubehag, som følge.

Gerningsindholdet har derfor et bredt defineret indhold, idet bestemmelsen rummer et forsæt til vinding, men dertil også handlingsforsæt alene til at påføre andre tab eller ulempe. Strafbestemmelsen forudsætter indirekte, at det er en person, som bliver vildledt og dermed ikke en maskine. Såfremt handlingerne vedrører et dataprogram, henføres det til strafbestemmelsen § 201.

I forarbejderne[100] til strl. § 202, følger, at det i norsk ret er strafbelagt at forsøge på (data)bedrageri, hvorfor der med denne kriminalisering er tale om en beskeden ny kriminalisering[101], "*men at der kan være et overlap mellem bestemmelserne, dog henfører de til selv om flere handlinger som kan tenkes om fattet av straffebudet om identitetskrenkelse i dag er straffbare som forsøk på andre*

[100] jf. Ot.prp nr. 22 (2008-2009)
[101] Jf. Ot.prp nr. 22 (2008-2009), side 44ff

forbrytelser, er det likevel et behov for bestemmelsen. Identitetskrenkelse kan krenke menneskers integritet og sikkerhet uavhengig av om den rent faktisk fører til videre lovbrudd eller ikke. Det vil også være enklere å bevise identitetskrenkelse enn (forsøk på) den fullbyrdete bedragerihandlingen".

Strafbestemmelsen i § 202 minder om strl. § 372, angående *'grovt bedrageri'*, men udvider strafansvarets betydning, idet der ikke forudsættes et misbrug af "identitetsbevis", hvorunder elektroniske dokumenter omfattes[102]. Såfremt der efter norsk ret kan idømmes straf efter begge delikter vil § 202 have forrang. Endvidere kan der, som kendt i dansk ret, statueres ansvar for forsøg og medvirken, og samtidig straffes i sammenstød, såfremt andre forbrydelser er forsøgt fuldført. Desuden indeholder § 202 adfærd, som kan idømme straf efter § 390 a, om krænkelse af privatlivets fred, hvorfor der er tale om en præcisering af retsområdet med denne ny kriminalisering.

Med strafbestemmelsen i § 202 vil brugen af anden samt en fiktiv identitet, være strafbelagt, såfremt den er let at forveksle med en anden identitet. Formålet med dette er at sikre, at der ikke er en gråzone i retspraksis, og forudsætter at kriminalisere de forhold, der har til hensigt at skabe vinding eller at påføre anden tab eller ulempe. Det fremgår af høringsinstansernes syn til det norske lovforslag[103], at ni instanser på den ene side, støttede forslag om kriminalisering, idet de fandt behov for strafbestemmelsen til at fange problemet, herunder de såkaldte phishingangreb.
På den anden side udtrykte adskillige afdelinger skepsis til kriminalisering af identitetstyveri. Særligt i forhold til afgrænsningen af brugen af urigtig og dermed en falsk identitet, som kan være et for snævert område[104] at definere, idet det ikke altid vil kunne defineres klart.
Endvidere fremgår det, at Finansnæringens hovedorganisasjon ønsker at afvente en nærmere behandling i EU før tiltag efterfølges. Hvorimod det norske Datatilsyn klart giver udtryk for, at handlingerne bør være ulovlig og dermed strafbelagt, og udtrykker, at brugen af en anden identitet alternativt kunne være et strafskærpende moment ved anden kriminel handling. Udvalget støtter op om behovet for regulering af området, særligt i forhold til en stjålet identitet, som benyttes på bekostning af andre, og understøtter herunder at "*bruken av uriktig identitet skal bare være*

[102] Jf. Forarbejder – Kapitel 21. Vern av informasjon og informasjonutveksling, side 237
[103] jf. Ot.prp nr. 22 (2008-2009), side 43, jf. pkt. 2.9.5
[104] Jf. Ot.prp nr. 22 (2008-2009), side 43, jf. pkt. 2.9.5

straffbar dersom bruken er uberettiget. Det skal ifølge utvalget tas hensyn til alminnelig nettvett, og om identiteten tillegges noen betydning i den aktuelle kommunikasjonen. Anbefalt bruk av fiktiv identitet, for eksempel i forbindelse med barns kommunikasjon på internett, er ikke ment å være omfattet"[105].

Departementet udtaler, at de ikke ser grund til at vente med en kriminalisering, da der er brug for en præcisering af retsområdet til beskyttelse af individernes identitet, idet en identitetskrænkelse kan påvirke ofret, uanset om der fuldbyrdes andre strafbare forhold. Udvalget oplyser, at strafbestemmelsen rummer en fiktiv identitetsmisbrug, og undlader derved at skulle definere gråzonen mellem identiteter, men udtrykker at regulere de forhold, hvor en anden identitet er let at forveksle. Dette er efter udvalgets antagelse lettere at definere. Hvorfor der med en ny kriminalisering ønskes en brugervenlig og informativ straffelov, som ikke går ud over, hvad der er nødvendig at kriminalisere. Departementet mener endvidere, at kriminaliseringen kan være med til at bekæmpe phishingangreb, som er et stigende problem, og skabe en større sikkerhed, idet disse angreb ofte benyttes som led til at begå identitetstyveri. Hvormed § 202 kriminaliserer identitetskrænkelse, som ofte er forudgående led til anden kriminalitet.

Hverken svensk eller dansk ret havde på daværende tidspunkt kriminaliseret identitetstyveri, eftersom det i dansk ret ikke fandtes klarlagt, om der konkret var behov for en sådan kriminalisering[106], og henfører til Bet 2002 1417, idet der var tvivl om en strafbestemmelse kunne præcisere de omtalte forhold og regulere strafområdet efter de tilsigtede formål.

I det norske departement lagde man til grund, at kriminaliseringen er med til at skabe tillid til internetbaseret handlinger, da reguleringen vil fremme og styrke krænkelser af den personlige integritet. Hvorfor Dansk Folkeparti i 2011 fremsatte et forslag til Folketingsbeslutning[107], jf. afsnit 4.1 samt 4.1.1, om en særskilt straf for identitetstyveri og identitetsmisbrug[108]. Et forslag, der var inspireret af den norske straffelov, dengang § 190 a nu § 202, som straffer den, der uberettiget

[105] Jf. Ot.prp nr. 22 (2008-2009), side 43, jf. pkt. 2.9.4
[106] Jf. Betænkning nr. 1417 af 2002 om it-kriminalitet, side 109f
[107] Jf. B 3 – 2011-12
[108] Jf. Trzaskowski, Jan: Internetretten, side 612

sætter sig i besiddelse af en andens identitet. Lovforslaget blev dog ikke vedtaget, hvorfor området endnu ikke er kriminaliseret i dansk ret.

4.2.2 Lag 2016:485 om ”olovlig identitetsanvändning” – Svensk straffelov

I 2015 blev lovforslaget om kriminalisering af identitetstyveri fremsat, hvorfor Sverige den 1. juli 2016 indsatte en ny strafbestemmelse om ”olovlig identitetsanvändning”, jf. BrB § 6 b:

” 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.”

Det fremgår af denne strafbestemmelse, under kapitel 4 i straffeloven om ”brott mot frihet och frid”, at de på samme måde som i norsk ret, kriminaliserer den, der uberettiget udgiver sig for at være en anden identitet, og omhandler identitetsoplysninger, herunder alt fra personnummer, adresse til billeder, der kan henføre og identificere et fysisk individ. Hvorfor beskyttelseshensynet i strafbestemmelsen udledes at være en fysisk levende persons identitet.
Det er derfor op til en konkret vurdering af hvert tilfælde at bedømme, om identitetsoplysningerne er tilstrækkelige for at identificere en bestemt person, hvorfor brugen af et navn antageligt ikke vil statuere et ansvar, men i kombination med andre oplysninger kan være tilstrækkelig. Her stilles ingen krav om, at oplysninger skal være korrekte, hvorfor fiktive informationer eller identiteter, som henfører til en anden, også som i norsk ret omfattes af strafbestemmelsen.
Endvidere stilles krav om, at brugen er uberettiget og dermed ulovlig, hvorfor handlinger begået ved samtykke fra pågældende identitet falder uden for strafbestemmelsen.

I strafbestemmelsen stilles krav om forsæt til at forårsage skade eller gener. Begrebet *skade* må derfor fortolkes til at omhandle en økonomisk skade og inkludere risiko for tab. Hvorved andet led henfører til ubehag eller ulempe, som ikke behøver at have et økonomisk afsæt, og stiller ligesom strl. § 202 krav om en vis bagatelgrænse af omfang. Således at det objektivt er tydeligt, hvorfor der alene stilles krav om, at skade eller gener ved brug af identitetsoplysninger kan tilskrives en effekt. Såfremt gerningsindholdet er opfyldt, kan gerningsmanden efter BrB § 6 b ifalde en straf med bøde

eller fængsel i op til 2 år[109], endvidere gælder, at der kan straffes i sammenstød for at udnytte flere identiteter.

Regeringen henfører, at indførelsen af en ny strafbestemmelse om ulovlig identitetsbrug kan sigte at modvirke identitetsmisbrug og ydermere stramme beskyttelsen mod krænkelse af privatlivets fred, idet ofret ved denne kriminalisering bedre kan udøve sin ret[110]. Heri ligger et ønske om at levere en tilstrækkelig beskyttelse af den enkeltes integritet, hvorfor Riksdagen udtrykker vigtigheden i at kriminalisere ulovlig identitetsbrug hurtigst muligt, jf. væddemål. 2014/15: JuU14, rskr. 2014/15: 138, idet der ikke i svensk strafferet forefindes en klar regulering af området, og da samfundsudviklingen hele tiden digitaliseres, øges sårbarheden for at begå misbrug af denne art[111]. Yderlig påpeges, at identitetstyveri har store konsekvenser, som følger alt fra praktiske til psykiske ulemper, idet ofrene er tvunget til at rapportere forbrydelserne og bestride krav. Hvorfor Regeringens ønske sammenholdes med EU-praksis, idet "staten har en positiv förpliktelse att vidtarimliga åtgärder för att skydda den enskildes privata sfär"[112], hvorfor man derved ønsker at kriminalisere en overtrædelse af den personlig integritet, idet det ikke er rimeligt, at nogen skal udholde skade, som følge af at en anden ulovligt udnytter identiteten.

I forarbejderne udtrykkes særligt problematikken ved phishing, herunder "*en företeelse som är starkt förknippad med olovlig identitetsanvändning är s.k. phishing, dvs. nätfiske eller lösenordsfiske*.", jf. *Allmänt om olovlig identitetsanvändning*, afsnit 4.1[113]. Endvidere beskrives af Polisens nationella bedrägericentrum, at bedrageri ved hjælp af identitetstyveri udgør en stor del af handlingerne, som har haft en progressiv stigning de seneste år, hvorfor vigtigheden af en kriminalisering kan statueres. Riksdagen finder derfor, at tiltag om kriminalisering af identitetstyveri er nødvendig. Særligt, da der ikke tidligere har været en klar definition af identitetstyveri i svensk ret.

Reguleringsgrundlaget bygger på de norske tiltag og kriminalisering af området, idet Danmark

[109] Jf. Betænkning nr. 1563 af 2017 om freds- og æreskrænkelser, side 276, jf. Prop. 2015/16:150, side 1
[110] Jf. Prop. 2015/16:150, side 1
[111] Jf. Prop. 2015/16:150, side 7, jf. pkt. 4.1
[112] Jf. Prop. 2015/16:150, side 13
[113] Jf. Prop. 2015/16:150, side 7, jf. pkt. 4.1

endnu ikke har ulovliggjort brugen af anden identitet. Forslaget bygger på at beskytte ageren på internettet på samme måde som strl. § 202, om at modvirke misbrug af identitetsoplysninger og øge beskyttelse mod dem, hvor privatlivet krænkes. I svensk ret gælder, på samme måde som dansk og norsk strafferet, at kriminelle handlinger kan henføres under andre bestemmelser i straffeloven. Hvorfor der henvises til den svenske strafferet kapitel 15, jf. BrB § 12, hvormed en modpart med forelæggelse af identitetsoplysningerne vildledes, ligesom den danske STRFL, § 171, angående dokumentfalsk. Da BrB § 12 ikke beskriver noget om ulovlig identitetsmisbrug, her identitetsanvändning, er der derfor brug for en præcisering af retsområdet.

Idet der i svensk ret også foreligger tilfælde, hvor identitetstyveri er et forudgående led til at begå anden kriminalitet, herunder særligt dokumentfalsk, er det derfor op til en konkret vurdering af domstolene, hvilken straf gerningsmanden skal ifalde, såfremt beskyttelseshensynene er forskellige. Såfremt der kan straffes i sammenstød, gælder efter svensk ret, at der idømmes straf for den af overtrædelserne med højeste straframme, med krav om at benævne identitetstyveri som del af citering[114].

4.3 Sammenfatning

Det kan af ovenstående udledes, at der i takt med at sårbarhederne øges, har været et større fokus på, at man nationalt tiltræder foranstaltninger for at beskytte individernes integritet, hvorfor Norge som foregangsland har indrammet denne kriminalisering med strl. § 202. Den norske straffelov § 202 angående ”*identitetskrenkelse”*, kriminaliserer således den der uberettiget anvender en andens identitet. I strafbestemmelsen stilles krav om forsæt til at opnå uberettiget vinding, ikke en økonomisk vinding, men forudsætter alene, at der er skabt en fordel hos modparten ved denne brug. Yderlig straffes handlinger, hvor det overvejende er sandsynligt, at det vil påføre en anden tab eller ulempe. Hvorfor strafbestemmelsen har et bredt beskyttelsesobjekt, hvilket er gennemgående, såvel i den norske som den svenske regulering af området, med indsættelse af strafbestemmelsen BrB § 6 b om ”olovlig identitetsanvändning”.

Forud for indsættelsen af en direkte kriminalisering gælder, at alle tre lande har kunne henføre dele af gerningsindholdet af identitetstyveri og identitetsmisbrug under andre bestemmelser i den

[114] Jf. Betænkning nr. 1563 af 2017 om freds- og æreskrænkelser, side 277

nationale straffelov. På baggrund af denne sondring udledes, at der er tale om en beskeden ny kriminalisering, hvorfor tiltaget har været "let" at implementere i henholdsvis norsk og svensk ret, idet databedrageri og dokumentfalsk på samme måde er strafbelagt, som efter det danske retssystem. Hvilket giver anledning til at antage, at samme vil gøre sig gældende ved implementering i det danske retssystem.
Til trods for at der har været uenigheder omkring selve udformning af strafbestemmelsen ved forudgående forhandlinger, så har flertallet i adskillige udvalg i henholdsvis Norge og Sverige fundet det nødvendigt at præcisere området, idet der har forelagt en gråzone omkring kriminaliseringen, og derfor har man støttet behovet for at beskytte ofrene, der uanset om anden kriminel handling fuldbyrdes, ofte er påvirket såvel psykisk som økonomisk, idet de skal rapportere og bestride krav.

Af ovenstående sammenfattes, at den norske regulering af området har haft indvirkning på de efterfølgende tiltag i svensk ret, her nærliggende også dansk ret, idet lovforslag i national ret er fremsat på baggrund af denne kriminalisering. Hvorfor det lægges til grund, at der er behov for en hensigtsmæssig regulering af strafområdet, idet der er behov for en præcisering uden at denne er for vidtgående. Det fremgår endvidere af forarbejder til strl. § 202, at der er tale om en beskeden ny kriminalisering, hvorfor der henføres til B 272 i det fremsættelsen af en lignende kriminalisering i dansk ret, må antages at have "*yderst begrænsende økonomiske konsekvenser*[115]", hvilket derved kan tale for, at fremme den strafferetlige beskyttelse af ofrene for identitetstyveri for dermed at præcisere retsområdet nationalt. Om ikke andet, kan en direkte kriminalisering være fordelagtig, idet det i forhandlingerne af både § 202 og § 6 b fremgår, at reguleringen understøtter bekæmpelse af phishingangreb, som globalt er et stigende problem, og dermed skaber en større sikkerhed, idet disse angreb ofte benyttes som led til at begå identitetstyveri.

[115] Jf. B 272 – 2020-21

Kapitel 5

5.1 Identitetstyveri på verdensplan

Af ovenstående udledes, at enkelte lande nationalt har iværksat tiltag til at regulere identitetstyveri. OECD udtaler dog, at der ikke er mange lande, som særkilt har implementeret en strafbestemmelse angående identitetstyveri, hvorfor retsområdet om identitetstyveri og identitetsmisbrug stadig fremgår uklar og forholdsvis ureguleret. OECD benævner særligt USA som foregangsland med kriminalisering af *ID-theft*, samt nordiske lande som Norge og Sverige, der selvstændigt har kriminaliseret ”*identitetskrenkelse”* samt ”*olovlig identitetsanvändning*”. Hvilket bringer os videre til at se på identitetstyveri i lyset af de seneste aktiviteter, idet der indledningsvis blev indikeret en antagelse om at COVID-19 pandemien har gjort markedet for cybercrime mere sårbart, hvorfor denne problemstilling nærmere belyses i forhold til de seneste hackingangreb med identitetstyveri, som følge.

5.1.1 COVID-19 pandemiens indvirkning på cybercrime

COVID-19 pandemien påvirkede verdenssamfundet drastisk, hvorfor flere lande ligesom Danmark, uge efter uge, gik i lockdown. Det medførte, at flere arbejdspladser pludselig stod overfor en omstillingsparathed, i forhold til at skulle tilpasse situationen med hjemmekontor, nye arbejdstilgange og dertil nye daglige levemåder. Verdenen over spredtes en utryghed og uvidenhed omkring pandemien, hvilket åbnede op for en del nye sårbarheder, set i lyset af hackere, der kunne udnytte denne menneskelige frygt, som anført: ”*During the COVID-19 pandemic, vulnerabilities manifested mainly as unknown flaws and weaknesses that attackers took advantage of, to compromise corporate data privacy and sensitive personal information*”[116].

Eksempel herpå er, at der i løbet af de første 6 måneder af 2019 blev tilgået 4.1 billion online arkiver[117], endvidere blev 4000 COVID-19 relaterede hjemmesider oprettet fra januar til marts måned 2020[118], og i løbet af 24 timer, fra den 14. til 15. april 2020, blev der modtaget 170.387 spam e-mails i det amerikanske marked, som indeholdt ordet ”corona” eller ”COVID”. Herunder blev 19.694 IP-adresser brugt til at afsende disse e-mails, samt 8.391 domain e-mails, hvoraf 583 e-mails

[116] Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 29
[117] Jf. Sangster, Mark: No safe Harbor, side 8
[118] Jf. Sangster. Mark: No safe Harbor, side 152

indeholdt ondsindede vedhæftninger[119]. Ovenstående eksempler viser, at hackere forsøgte at udnytte den kritiske verdenssituation, idet de gennem SE som deres *entry point,* tilegnede sig personlige informationer [120] omkring de pågældende individer. Hvorfor en ellers hensigtsmæssig nedlukning for at indramme virussen, påvirkede markedet for cybercrime i en negativ retning, idet det muliggjorde andre indgangsvinkler til cyberangreb, som gentagne gange medførte større kompromitteringer af identitetsoplysninger, som følger.

Den 17. april 2020, oplevede 20 millioner profiler til Aptoide et databrud og dertilhørende læk af informationer[121]. Senere samme måned, oplevede japanske Nintendo frem til juni 2020, at være offer for hackerangreb. Først blev 160.000 profiler kompromitteret. Et tal, der dernæst steg med 140.000 profiler, hvorigennem identitetsoplysninger til 300.000 profiler[122] blev lækket. Endvidere blev Twitter hacket, hvorunder 130 velkendte personer blev kompromitteret, herunder navne som Barack Obama, Bill Gates, Elon Musk[123] mv.
Det kan af ovenstående tilfælde udledes, at der internationalt har været en markant stigning i cyberangreb, som følge af lockdown, idet flere og flere har søgt til brugen af teknologiske midler, der ikke har samme it-sikkerhed og dermed øget muligheden for databrud.
Sammenholdes data med mulige phishingangreb, så udledes det, at antallet af phishingangreb under pandemien havde en drastisk stigning på hele 400 pct.[124] Fælles for disse cyberangreb var den emotionelle tilgang med udnyttelse af de menneskelige instinkter og manglende information omkring pandemien, hvormed frygt blev udnyttet som indgangsvinkel til at stjæle identitetsoplysninger.

I en dansk kontekst, har særligt de omtalte NemID-sager været i fokus, hvorfra der senest, den 12. maj 2021[125], af Danmarks Radio, er bragt nyheder om NemID svindel. En sag, hvor 6000 CPR-numre blev fundet hos terrordømt, hvorunder 170 individer har fået misbrugt deres identitetsoplysninger, som omfatter et tocifret millionbeløb. I sagen har gerningsmændene

[119] Jf. United Nations Office on Drugs & Crime: COVID-19: Cyber Threat Analysis – cybercrime program.
[120] Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 85 + 116.
[121] Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 76-78
[122] Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 79
[123] Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 34+68
[124] Jf. Cole, Dr. Erik: "Phishing: You Are A Target"
[125] Jf. Dr.dk: "Vildledende" og "mangelfuld"

rutinemæssigt tjekket skattemapper, optaget lån, hævet penge, ændret NemKonto, og derved fuldbyrdet databedrageri ved hjælp af installation af keyloggere på offentlige biblioteker, hvorfor sagen behandles under STRFL § 279a. Ofte indestår bankerne for tab ved misbrug af NemID, men alt andet lige står forurettede tilbage med en aftaleretlig forpligtelse i forhold til de indgåede lånforhold, som de skal bestride overfor fogedretten, jf. afsnit 3.5.

Der tegner sig derfor et billede af usikkerhed, når det kommer til håndtering af svindelsager med identitetsoplysninger, idet det af ovenstående må fastsættes at være et internationalt problem. Hvorfor det kan udledes, at COVID-19 pandemiens cyberangreb har udviklet sig hastigt med sofistikerede angreb, idet hackerne har udnyttet de digitale sårbarheder, som pandemien indirekte efterlod, og det har ikke været muligt at lave *last minute* ændringer for at sikre og beskytte de pågældende data. Samtidig har det efterladt en usikkerhed omkring håndtering af data på internettet, idet *"most of the online frauds that took place during the pandemic centred around malicious hackers who were able to manipulate innocent people"*[126], hvorfor det forventes at antallet af cyberangreb vil have en fortsat eksponentiel udvikling i 2021, og antagelsen om pandemiens indvirkning må besvares som værende korrekt.

5.1.2 År 2021-2025

I sammenspil med internettets hastige udbredelse og national digitalisering, vil det alt andet lige være hensigtsmæssigt at se på de nye alternative sårbarheder, som øges, for bedst muligt at regulere retstilstanden på området, idet der hvert 39 sekund forekommer et cyberangreb, og da omkostninger herfor antages at stige fra $6 trillioner (USD) i 2021, og $10.5 trillioner (USD) i 2025, belyses vigtigheden heraf.

Af ovenstående udledes, at området fortjener anerkendelse på verdensplan, da en global cyber-awareness kan skabe samarbejde på flere niveauer, som vil øge sikkerheden og tiltro til brugen af internettet, som helhed. Endvidere vil det imødekomme problemet med jurisdiktion, såfremt der kan udarbejdes ensartede direktiver og tiltag til regulering og forebyggelse af identitetstyveri og identitetsmisbrug.

[126] Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 68

På nuværende tidspunkt foreligger der et cybercrime-direktiv[127], nærmere Direkte 2013/40/EU, som erstatter 2005/222/RIA. Et direktiv om angreb på informationssystemer, som ikke er bindende for eller finder anvendelse i Danmark. Dog står Danmark overfor udvikling af 5G netværk, hvorfor CFCS er med inde over drøftelserne angående it-sikkerheden. De har blandt andet opstillet et *afbødningstiltag for at modvirke og modgå risikovurdering identificerede risici ved 5G netværk* [128], som er med til at optimere mere sofistikeret sikkerhedsværktøjer. Idet samfundet lever under det fænomen, at det nærmest er umuligt ikke at have efterladt et digitalt spor gennem handlinger eller transaktioner[129] på internettet, er Danmark derfor del af den nye cybersikkerhedsverificering, som skal være i drift senest juni 2021. Der er tale om en certificering, gennem den nye *cybersikkerhed forordning* for informations- og kommunikationsteknologi, der nationalt tilsigter at øge den digitale sikkerhed. Certificeringen bevirker, at virksomheder kan få certificeret deres produkter, tjenester og processer med et certifikat gældende på tværs af medlemslandene. Det er Erhvervsministeriet, der står for denne etablering[130], som udtrykker, at det er et bud på en mere sikker tilgang til at begå sig på internettet. Hvorfor det er vigtigt, at man fortsat opdaterer tiltag efter de nye standarder, så der ikke skabes en mistillid, som ved de benævnte NemID-sager.
Yderlig, er *Domain-based Message Authentication, Reporting and Conformance* udarbejdet, som skal gøre e-mail kommunikation, og derved mail brugen mere sikker, med henblik på at reducere phishingangreb, idet afsenderadressen får tilføjet et certifikat, som er vanskeligt at manipulere[131].

Afsluttende må det konkluderes, at den kommende periode vil være afgørende for at oprette de rette rammer for en international, herunder national, cybersikkerhed. Idet den kommende periode vil karakterises af de nye tiltag og værktøjer, der på baggrund af de seneste COVID-19 relaterede angreb er udviklet for at optimere cybersikkerhed og bekæmpe hackingangreb, som identitetstyveri[132].

[127] Jf. Justitsministeriet: Notat om tilvalg af cybercrime-direktivet, jf. direktiv 2013/40/EU
[128] Jf. CFCS: Beretning 2019, side 27
[129] Jf. Sztandarowski, Lucas: The real cybercrime, side 23f
[130] Jf. CFCS: Beretning 2019, side 26
[131] Jf. Sikkerdigital.dk: DMARC (anti-phishing)
[132]Jf. Okereafor, Kenneth: Cybersecurity in the COVID-19 pandemic, side 125

Kapitel 6

6.1 Konklusion

Den teknologiske udvikling har nødvendiggjort en elektronisk privatsfære, hvorfor der i 1985 blev indsat regler om datakriminalitet i straffeloven, hvortil nye beskyttelsesobjekter med oplysninger blev indsat, med en sikring af databehandling i STRFL § 263 om hacking samt bedrageri, her særligt databedrageri i STRFL § 279a.

Identitetstyveri omhandler i kandidatspecialet, det, at *nogen ulovligt tilegner sig en andens oplysninger*, *og/eller at nogen misbruger disse oplysninger.* Som alt overvejende hovedregel må der i dansk ret konkluderes, at identitetstyveri ikke er strafbart, medmindre handlingerne vedrører andre delikter, og gerningsindholdet matcher den pågældende strafbestemmelse, og dermed opfylder de konkrete strafbarhedsbetingelser for at ifalde straf. Derfor gælder, at en anmeldelse om et identitetstyveri alt efter omfang og alt efter fremgangsmåde, vil kunne straffes efter STRFL §§ 171, 263, 276 og 279.

Første led vedrører tilegnelse, som efter straffeloven kan tilfalde straf efter hacking- og tyveribestemmelsen, hvorfor det kan medføre enkelte overvejelser i forhold til sondringen om, identitetsoplysninger er en offentlig tilgængelig information om en identitet, eller der er tale om en handling, hvor der skaffes en adgang, som efter STRFL § 263 vil være strafbart, og uanset udfaldet kan formålet med adgangen have betydning for strafudmålingen, og dermed være en formildende eller skærpende omstændighed.

Såfremt identitetsoplysninger er borttaget uden samtykke fra besidderen, vil det henføre under tyveribestemmelsen. Hvortil det kan skabe forvirring om et individs identitet, kan være genstand for sådan en borttagelse af en fremmed rørlig ting, og stille supplerende spørgsmål ved om identiteten har en reel materiel værdi. Af ovenstående analyse udledes, at identitetsoplysninger er tilknyttet et fysisk objekt, hvorfor det konkluderes, at disse oplysninger kan borttages og dermed stjæles, idet de har en omsættelig værdi på det illegale marked, og indgår derfor af ordlyden i strafbestemmelsen. Yderlig kan der ved tyveri være tale om nødværge situation, hvilket i en digital kontekst må konkluderes at være vanskelig, idet manglende fastlæggelse af retspraksis mangler.

Såfremt der ikke er tale om en ulovlig tilegnelse eller borttagelse, kan de efterfølgende handlinger, som dokumentfalsk og bedrageri, være strafbelagt.
Der kan være tale om, at identitetsmisbruget omhandler handlinger, der bevirker at skuffe i retsforhold, hvorved det viljemæssige er indforstået, at man vildleder modparten ved at overgive eller forevise dokumenter. I sådanne tilfælde vil handlingerne være omfattet af dokumentfalsk efter STRFL § 171. Endvidere kan der være tale om en vildfarelse, som kan ske, enten ved kontakt med gerningsmanden, jf. STRFL 279 eller gennem en elektronisk databehandling, jf. STRFL § 279a. Hvorfor der stilles krav om, at identitetstyveri skal bevirke en handling eller undladelse, der er fremkommet ved en vildfarelse, hvorfra der ved modparten skal foreligge en disposition, og dermed et valg om at aktualisere et motiveret grundlag, som på baggrund af den pågældende vildledelse ville have undladt.

Strafferammen vil i pågældende tilfælde, alt efter gerningsindhold, kunne straffes med bøde eller fængsel i op til 1 år og 6 måneder, jf. STRFL § 263, § 276 og under særligt skærpende omstændigheder kan straffen stige til 6 år, jf. STRFL § 263 stk. 3, samt § 285, jf. § 276. Endvidere vil strafferammen for identitetsmisbruget kunne ifalde bøde eller fængsel i op til 2 år, jf. STRFL § 171, og i særligt grove tilfælde op til 6 år, jf. § 172. Hvormed STRFL § 279 straffes med bøde eller fængsel i op til 1 år og 6 måneder, jf. § 285, og nærmere op til 8 års fængsel, hvis der er tale om forsætligt eller groft uagtsomhed, som bevirker vildfarelsen, jf. STRFL § 300a. Hvorledes de enkelte handlinger skal subsumeres angår selve gerningsindholdet og mere konkret, hvordan identitetstyveri bliver realiseret, hvorfor der ofte idømmes straf i sammenstød for overtrædelse af straffelovens delikter.

Det må derved konkluderes, at identitetstyveri ikke i sig selv er strafbelagt, men da gerningsindholdet matcher andre bestemmelser i straffeloven, er disse handlinger strafbelagt med bøde eller fængsel op til 8 år. Grundet manglede regulering og præcisering af retsområdet, må der udledes, at retstilstanden på området er delvis uklar, idet der foreligger begrænset retspraksis. Da identitetstyveri og identitetsmisbrug ikke selvstændigt er kriminaliseret, kan der forekomme gråzoner i det strafferetlige værn, hvorfor det er op til en konkret vurdering ved domstolene at klarlægge praksis.

Når strafområdet er fastlagt, er det vigtigt også at sondre på beskyttelseshensynet ved retstilstanden i forhold til de aftaleretlige forpligtigelser, som forurettede kan ifalde. Hvorfor det af analysen fremgår, at det er op til en konkret vurdering af hændelsesforløbet, for at vurdere om individerne hæfter, og bliver aftaleretligt forpligtet. Sondringen angår, under hvilke omstændigheder tilegnelsen er sket, om der er kendskab til besiddelse af personidentificerbare oplysninger, samt hvad der er gjort for at minimere risici og forhindre misbrug. Det op til en konkret vurdering af omstændighederne, om der findes grundlag for at bestride disse krav, eller om forurettede har handlet med en sådan grad af uagtsomhed, at denne ifalder den aftaleretlige forpligtigelse.

Sammenholdes reguleringen med norsk og svensk ret, fremgår at Norge har været foregangsland, idet de selvstændigt har kriminaliseret ” identitetskrenkelse”, jf. strl. § 202, hvorefter Sverige har indsat ”olovlig identitetsanvändning”, jf BrB § 6 b med en straframme på 2 år. Herefter er der i Danmark forsøgt at fremsætte beslutningsforslag, som forventet skal have en præventiv effekt, og dermed sende et signal om, at det er ulovligt at stjæle og svindle med andres identiteter. B 186 henviser til den norske kriminalisering af området, idet den norske straffelov kriminaliserer den, der krænker en identitet, herunder stilles særligt et krav om forsæt til at opnå uberettiget vinding, eller det at påføre en anden tab eller ulempe. Såfremt det er overvejende sandsynligt, at handlingerne vil påføre nogen tab, vil dette også statuere et sådant ansvar, efter indholdet i strl. § 202. Det er endvidere vigtigt at bemærke, at der efter norsk ret statueres ansvar, såfremt gerningsmanden opnår en fordel, hvorfor der ikke stilles direkte krav til vindings- eller skadeshensigt, andet end en bagatelgrænse og hermed, at forholdet skal rumme en ulempe, der er højere end forurettes ubehag, som følge.
Endvidere udledes det, at det i norsk ret er strafbelagt at forsøge på (data)bedrageri, på samme måde som identitetstyveri efter strafbetingelserne kan henføres under dokumentfalsk i svensk ret, hvorfor der med denne kriminalisering er tale om en beskeden ny kriminalisering. En kriminalisering, hvorfra man lettere kan ifalde straf efter ”identitetskrænkelse”, og hermed identitetstyveri, fremfor fuldbyrdet bedrageri.
Endvidere lægges til grund, at det norske departement udtaler, at de ikke ser grund til at vente med en kriminalisering, grundet behov for proportional, brugervenlig og informativ regulering af

retsområdet til beskyttelse af individernes identitet. Da en identitetskrænkelse kan påvirke ofret, uanset om der fuldbyrdes andre strafbare forhold, hvilket understøttes af B 272. Beslutningsforslaget påpeger nemlig det højaktuelle behov for en regulering, som kriminaliserer identitetstyveri, også selvom der ikke er sket et efterfølgende identitetsmisbrug. Forslaget anfægter endvidere de pågældende huller i det strafferetlige værn, særligt usikkerhed omkring omfang og selve behandling af sager, der anmeldes.

Udbredelsen af den digitale teknologiske verden har medvirket til, at man lettere overskrider privatsfæren, hvorfor kriminalitet mod informationer er undergivet samme strafferamme som mod mere traditionelle værdier, herunder penge og fysiske objekter. I en digital tidsalder, må det alt andet lige konkluderes, at truslen fra cyberangreb ikke kan elimineres, hvorfor der i takt med internettets hastige udvikling er behov for både cyber- og informationssikkerhed, så samfundet fortsat kan drage positiv nytte af den teknologiske udvikling, og samtidig sikre at beskyttelsesobjektet er tilpasset udviklingen, herunder at privatlivets fred er beskyttet.

Idet der foreligger begrænset retspraksis til kriminalisering af identitetstyveri og identitetsmisbrug, vil der være betydelige gråzoner i dens anvendelse, som vil blive formindsket, i takt med at retstilstanden klarlægges, hvorfor en passende kriminalisering bør tilskyndes, så man i samfundet kan leve trygt med udfordringerne.

Kapitel 7

7.1 Afsluttende bemærkninger

Hidtil har der ikke været et politisk flertal for, at identitetstyveri bliver et selvstændigt begreb i straffeloven. Om begrebet får en særskilt strafbestemmelse, vil derfor være op til et politisk flertal efter de nye forhandlinger.

Kandidatspecialet afsluttes med bemærkning om, at B 272 om kriminalisering af identitetstyveri og identitetsmisbrug er fremsat behandling den 18. maj 2021.

Litteraturliste

*Artikler, lovgivning og retspraksis er hentet fra Karnov.dk, hvorfor denne tilgang gennem opgaven er benyttet.

Lovgivning

- Lovbekendtgørelsen 2020-11-17 nr. 1650 - **Straffeloven**
- Lov 19 juni 2009, nr. 74 - **Lov om Straff** - Norsk straffelov
  Link: https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_2-6#§202
- Lag 2016:485 - **Brottsbalk**- Svensk straffelov
  Link: https://lagen.nu/1962:700#K4P6b

Forarbejder:

- Forarbejder til norsk straffelov - **Ot.prp nr. 22 (2008-2009)**
  Link:https://www.regjeringen.no/contentassets/10118c83df37474e9c61e86765c7af98/no/pdfs/otp200820090022000dddpdfs.pdf
- Forarbejder til svensk straffelov - **Prop. 2015/16:150 – 2016**
  Link:https://www.regeringskansliet.se/49568e/contentassets/59bfb1c11a234a8c87bd5600d9037a73/151615000webb.pdf?TSPD_101_R0=082953afa5ab20008f4d692588ca3bf10fb2668fd563df313505fb383e87a93754cda98803d32454088814f2eb1430000739fd4130cbec7b717b1539d8d9cc3e028d0e0226b3adae37ac2b384cc3481c9a9b8ced3372e356f001a5e913b6ed6d

Lovforslag:

- **Beslutningsforslag B 272**: Forslag til folketingsbeslutning om kriminalisering af identitetstyveri og identitetsmisbrug, fremsat 9. marts 2021.
  Link:https://www.ft.dk/ripdf/samling/20201/beslutningsforslag/b272/20201_b272_som_fremsat.pdf
- **Beslutningsforslag af B186**: Forslag til folketingbeslutning om en særskilt straf for identitetstyveri og identitetsmisbrug, fremsat 13. april 2016.

Link:https://www.ft.dk/samling/20151/beslutningsforslag/b186/20151_b186_som_fremsat.htm

- **Beslutningsforslag B 100:** Forslag til folketingsbeslutning om styrket beskyttelse af personnummeret.
  Link: https://www.ft.dk/samling/20121/beslutningsforslag/b100/index.htm
- **Beslutningsforslag B 3:** Forslag til folketingsbeslutning om en særskilt straf for identitetstyveri og identitetssvindel.
  Link: https://www.folketingstidende.dk/samling/20111/beslutningsforslag/B3/index.htm

Borgerforslag:

- **Kriminalisering af identitetstyveri I § 264 e** – link: https://www.borgerforslag.dk/se-og-stoet-forslag/?Id=FT-07807

Betænkning:

- **Betænkning nr. 1032** af 1985 om datakriminalitet
- **Betænkning nr. 1417** af 2002 om it-kriminalitet
- **Betænkning nr. 1563** af 2017 om freds- og ærekrænkelser

Direktiv:

- **Directive 2013/40/EU** on attacks against information systems, 12. august 2013
- Justistsministeret.dk: **Justitsministeriets notat om tilvalg af cybercrime-direktivet** særligt direktiv 2013/40/EU - Link: https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2015/Bilag%205%20-%20Cybercrime-direktivet.pdf (Tilgået senest den 23. april 2021)

Retspraksis:

Ugeskrift for retsvæsen:

- AFGR.2021-0226-4
- U.2021.1268
- U.2021.1166
- U.2020.4284
- U.2020.3899
- U.2020.2771
- U.2019.1192
- U.2019.1197
- U.2018.993
- U.2018.1787
- U.2016.2074
- U.2016.1145/2H
- U.2016.2074Ø
- U.2015.3615Ø

Tidskrift for kriminalitet:

- TfK2021.313
- TfK2021.298
- TfK.2019.1411
- TfK2018.575/1
- TfK2016.484/1
- TfK2018.138/1

Teleankenævnet:

- Den 8. marts 2018, sag: 17-91 - Link: https://teleanke.dk/wp-content/uploads/2019/04/17-91.pdf
- Den 3. maj 2010, sag 17-212 - Link: https://teleanke.dk/wp-content/uploads/2019/04/17-212.pdf

Dansk litteratur:

- Munk-Hansen, Carsten: **Retsvidenskabsteori**, 2. udgave, 1.oplag, Djøf Forlag, 2018.
- Toftegaard Nielsen, Gorm, Thomas Elholm & Morten Niels Jakobsen: **Kommenteret Straffelov, Speciel del**, 11. udgave, Jurist- og Økonomforbundets Forlag, 2017
- Udsen, Henrik: **IT-ret,** 4. udgave, Ex Tuto Publishing A/S, 2019.
- Trzaskowski, Jan(red.), Søren Sandfeld Jakobsen, Susanne Karstoft, Hanne Kirk, Lars Bo Langsted, Thomas Riis, Charlotte Bagger Tranberg & Helena Lybæk Gudmundsdóttir: **Internetretten**, 3. udgave, Ex Tuto Publishing A/S, 2017.
- Waaben, Knud: **Strafferettens specielle del**, 6. udgave, Karnov Group Denmark A/S, 2014.

Engelsk litteratur:

- A. Gillespie, Alisdair: **Cybercrime – Key Issues and Debates**, 2. edition., Routledge, 2019
- Cole, Dr. Eric: **Phishing You Are A Target,** Secure Anchor, safeguarding the digital world, 2020.
- Okereafor, Kenneth: **Cybersecurity in the covid-19 pandemic**, 1. edition, CRC Press, Taylor & Francis Group, 2021.
- Richardson, Matthew: **Cybercrime- Law and Practice**, 1. edition, Wildy, Simmonds & Hill Publishing, 2019.
- Sangster, Mark: **No safe harbor**, 1 edition. Page two, 2021.
- Slade, Robert: **Cybersecurity lessons from COVID-19**, CRC Press, Taylor & Francis, 2021
- Sztandarowski, Lucas: **The Real Cybercrime**, 1 edition, Cyberdeffenseur Editions, 2020.

Artikler:

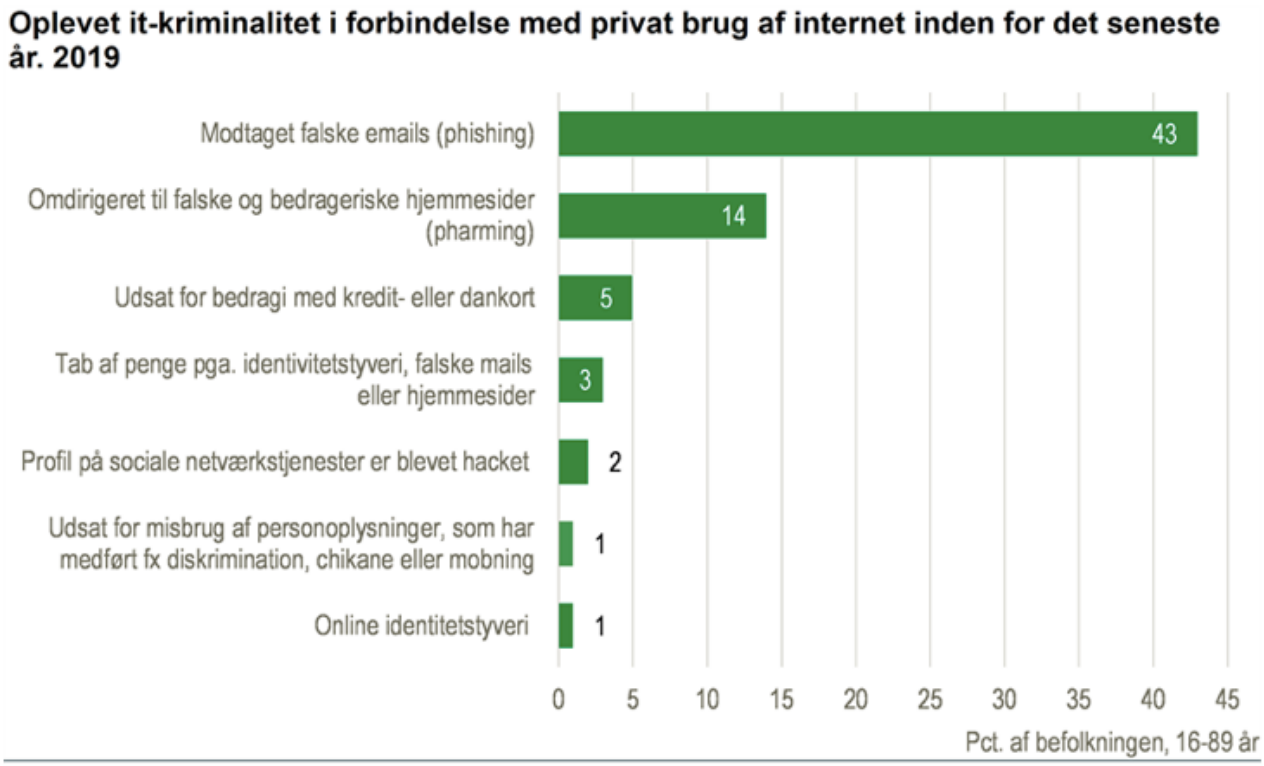
- Aalborg Universitet, Lene Wacher Lentz: **Hacking en forbrydelse eller digitalt selvforsvar** – link: https://vbn.aau.dk/ws/portalfiles/portal/402917035/3_2020_8.pdf
  (Tilgået senest den 20. april 2021)
- Borger.dk, skrevet af digitaliseringsstyrelsen: **Hvad er identitetstyveri** - link: https://www.borger.dk/internet-og-sikkerhed/Identitetstyveri/Hvad-er-identitetstyveri
  (Tilgået senest den 12. marts 2021)

- Borger.dk, skrevet af digitaliseringsstyrelsen: **Offer for identitetstyveri** – link: https://www.borger.dk/internet-og-sikkerhed/Identitetstyveri/Offer-for-identitetstyveri (Tilgået senest den 20. marts 2021)
- CFCS: **Center for Cybersikkerheds beretning 2029** - Link: https://cfcs.dk/globalassets/cfcs/dokumenter/beretning/-cfcs-beretning-2019-.pdf (Tilgået senest 11. maj 2021)
- Cybersecurityventures: **Cybercrime To Cost The World $10.5 Trillion Annually By 2025** - Link: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Tilgået senest den 1. april 2021)
- Danmarks Statistik: **Halvdelen har oplevet it-sikkerhedsproblemer** - Link: https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=41944# (Tilgået senest den 3. maj 2021)
- Danmarks Statistik: **Stigning i anmeldt bedrageri** – link: https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=30212 (Tilgået senest den 12. april 2021)
- Det Juridiske Fakultet, Københavns Universitet: **Internet Kriminalitet 2017** – Link: https://emu.dk/sites/default/files/2019-05/Internetkriminalitet%202017.pdf (Tilgået senest 28. april 2021)
- Det Kriminalpræventive råd: **Faktaark om identitetstyveri** – Link: https://www.yumpu.com/da/document/read/22879268/faktaark-om-identitetstyveri-politiets
- Det Kriminalpræventive råd: **It-kriminalitet i tal** - Link: https://dkr.dk/it/it-kriminalitet-i-tal/ (Tilgået senest den 10. april 2021)
- Det Kriminalpræventive råd: **Cybercrime – når kriminaliteten rykker online** https://www.dkr.dk/media/6921/cybercrimefolder2018.pdf (Tilgået senest 28. april 2021)
- Digitaliseringsstyrelsen: **Danmarks Radios historier om identitetstyveri og misbrug af NemID er misvisende og skaberutryghed på fejlagtiggrundlag** - Link: https://digst.dk/nyheder/nyhedsarkiv/2021/februar/danmarks-radios-historier-om-identitetstyveri-og-misbrug-af-nemid-er-misvisende-og-skaber-utryghed-paa-fejlagtigt-grundlag/ (Tilgået senest den 14. maj 2021)

- Danmarks Radio: **”Vildledende” og ”mangelfuld”: Hård kritik af redegørelse om NemID-svindel** – link: https://www.dr.dk/nyheder/indland/vildledende-og-mangelfuld-haard-kritik-af-redegoerelse-om-nemid-svindel (Tilgået senest den 13. maj 2021)
- European Commission: **Cybercrime** – link: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (Tilgået senest den 3. april 2021)
- Forbrug.dk (Konkurrence og Forbrugsstyrelsen: **Forbrugere hæftede for misbrug af deres NemID** – Link: https://www.forbrug.dk/nyheder/forbrug/2019/forbrugere-haeftede-for-misbrug-af-deres-nemid/
  (Tilgået senest den 10. marts 2021)
- Malwarefox, 2019: **Types of Hackers You Should Know** - Link: https://www.malwarefox.com/types-of-hackers/ (Tilgået senest den 25. marts 2021)
- Nasdaq: **5 Largest Economies In The World And Their Growth In 2020** - Link: https://www.nasdaq.com/articles/the-5-largest-economies-in-the-world-and-their-growth-in-2020-2020-01-22 (Tilgået senest den 1. april 2021)
- OEDC, 2007, **Scoping Paper on Online Identity Theft** - Link: http://www.oecd.org/sti/40644196.pdf (Tilgået senest den 28. marts 2021)
- Sikkerdigital.dk: **DMARC (anti-phishing)** – Link: https://sikkerdigital.dk/myndighed/tekniske-tiltag/dmarc/ (Tilgået senest den 15. maj 2021)
- UNODC (United Nations Office on Drugs and Crime): **COVID-19: Cyber Threat Analysis** – Link: https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf (Tilgået senest den 10. maj 2021)

Bilagsoversigt

Bilag 1:

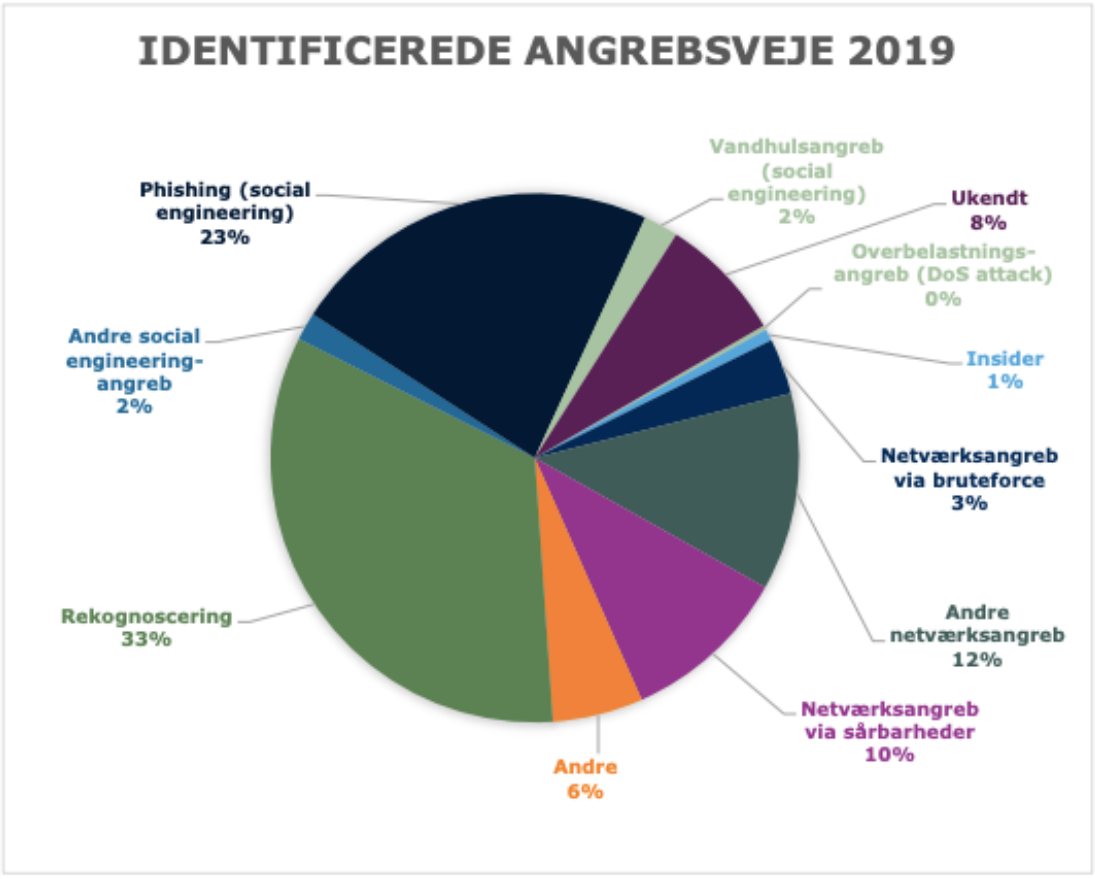


Danmarks Statistik: **Oplevet it-kriminalitet i forbindelse med privat brug af internet inden for det seneste år 2019** - Link: https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=41944

(Tilgået senest den 22. februar 2021)

Bilag 2:

Identificerede angrebsveje 2019



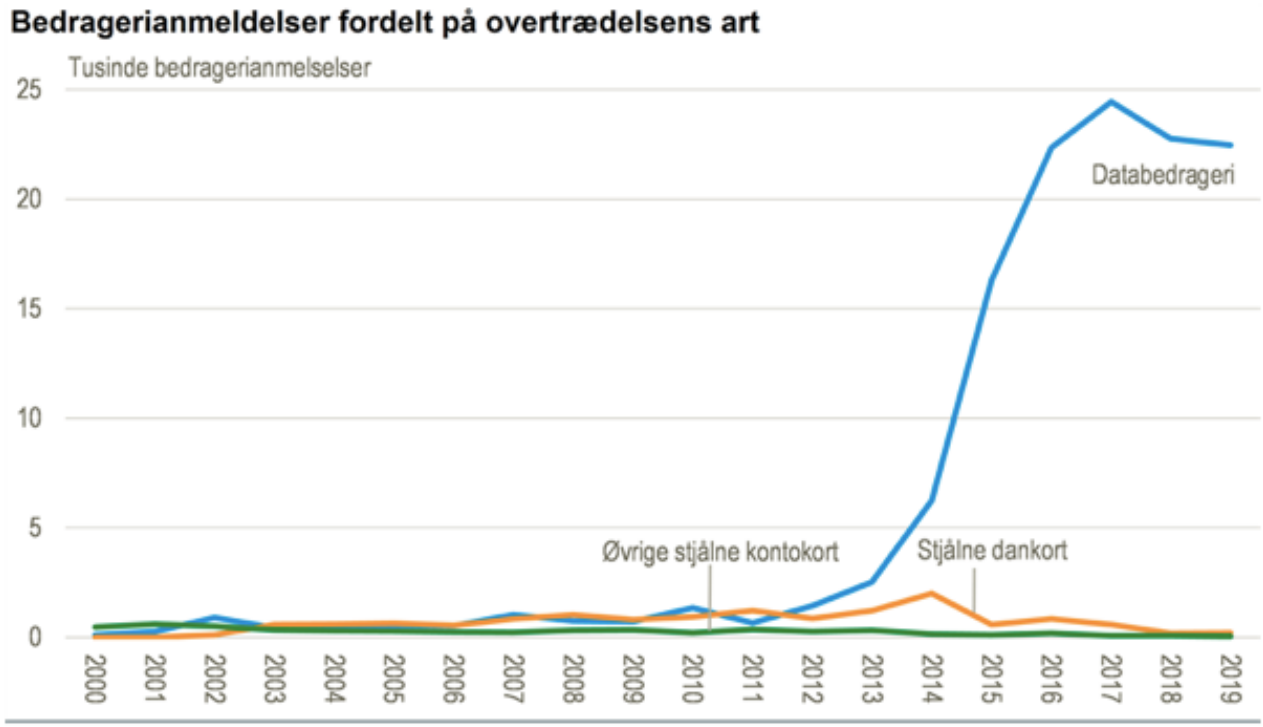
Kilde: Netsikkerhedstjenesten. Diagrammet viser de angrebsveje, det har været muligt at identificere ud fra CFCS' registrering. Diagrammet rummer potentielt falske positiver. Kategorien "Ukendt" dækker over hændelser, hvor det ikke har været muligt at identificere angrebsvejen.

CFCS: I**dentificerede angrebsveje 2019** - Link:

https://cfcs.dk/globalassets/cfcs/dokumenter/beretning/-cfcs-beretning-2019-.pdf

(Tilgået senest den 25. februar 2021)

Bilag 3:



Danmarks Statistik: **Bedragerianmeldelser fordelt på overtrædelsens art** – Link:

https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=41944

(Tilgået senest den 20. februar 2021)

Bilag 4:

Anmeldte forbrydelser og sigtelser efter anmeldte og sigtede, overtrædelsens art og tid

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Anmeldt											
Dokumentfalsk	2 247	3 269	2 448	2 423	2 282	2 418	2 924	2 789	2 178	2 313	2 566
Bedrageri	9 499	12 167	11 392	14 510	18 769	32 062	40 188	44 550	43 617	48 348	54 583
Sigtelser											
Dokumentfalsk	1 765	2 812	1 995	1 985	1 880	1 892	2 226	1 612	1 279	1 478	1 892
Bedrageri	5 691	7 770	7 348	8 208	10 900	15 480	18 189	17 537	15 448	15 074	22 032

Danmarks statistik: **Anmeldte forbrydelser og sigtelser efter anmeldte sigtede overtrædelsens art og tid** - Link: https://www.statistikbanken.dk/straf20

(Tilgået senest den 20. februar 2021)

Bilag 5:

1. Kvartal - 2021

Kriminalitet fordelt på aktiviteter

Periode	Aktivitet	Politikreds	Antal anmeldelser	Antal anmeldelser pr 1.000 indbyggere	Antal sigtelser	Sigtelsesprocent
2021 - 1. Kvartal	Økonomisk kriminalitet	Danmark i alt	15.306	2,6	14.125	92,3%
		Nordjylland	630	1,2	1.000	158,7%
		Østjylland	668	1,1	665	99,6%
		Midt- og Vestjylland	419	0,7	736	175,7%
		Sydøstjylland	1.248	2,5	1.530	122,6%
		Syd- og Sønderjylland	477	1,1	736	154,3%
		Fyn	458	0,9	831	181,4%
		Sydsjælland og Lolland-Falster	655	1,7	1.034	157,9%
		Midt- og Vestsjælland	492	1,1	746	151,6%
		Nordsjælland	729	1,2	844	115,8%
		Københavns Vestegn	1.203	2,9	1.369	113,8%
		København	8.307	10,4	4.616	55,6%
		Bornholm	20	0,5	18	90,0%

Helår - 2020

Kriminalitet fordelt på aktiviteter

Periode	Aktivitet	Politikreds	Antal anmeldelser	Antal anmeldelser pr 1.000 indbyggere	Antal sigtelser	Sigtelsesprocent
2020 - Helår	Økonomisk kriminalitet	Danmark i alt	64.675	11,1	60.270	93,2%
		Nordjylland	2.678	5,1	2.881	107,6%
		Østjylland	4.210	7,0	3.313	78,7%
		Midt- og Vestjylland	3.375	5,8	3.408	101,0%
		Sydøstjylland	3.015	6,2	3.581	118,8%
		Syd- og Sønderjylland	2.549	5,8	2.252	88,3%
		Fyn	2.883	5,8	3.761	130,5%
		Sydsjælland og Lolland-Falster	1.573	4,2	2.859	181,8%
		Midt- og Vestsjælland	2.447	5,3	3.744	153,0%
		Nordsjælland	3.507	5,9	3.701	105,5%
		Københavns Vestegn	4.732	11,3	5.456	115,3%
		København	33.568	42,3	25.166	75,0%
		Bornholm	138	3,5	148	107,2%

Danmarks politi database: **Kriminalitet fordelt på aktiviteter, særligt økonomisk kriminalitet** -

Link:https://statistik.politi.dk/QvAJAXZfc/opendoc.htm?document=QlikApplication%2F2999_Public%2FPublic_IndsatsResultater.qvw

(Tilgået senest den 18. maj 2021)


Ordoptælling
Statistik:
Sider 61
Ord 21.002
Tegn (uden mellemrum) 123.123
Tegn (med mellemrum) 143.994
Afsnit 371
Linjer 1.808
Medtag fodnoter og slutnoter
Luk