

Digital berigelseskriminalitet

Kandidatspeciale 2023

Aalborg Universitet
Cand.merc.jur.



Udarbejdet af:

Mikkel Adelsten Nielsen

Studienummer: 20183081

Telefonnummer: 27624788

Bo Jakobsen

Studienummer: 20184093

Telefonnummer: 22985788

Signe Zeidler Holm Andresen

Studienummer: 20186044

Telefonnummer: 23253362

Vejleder: Caroline Hornum Martinussen



**AALBORG
UNIVERSITET**

Abstract

This thesis aims to examine the legal safeguard against digital acquisitive crimes in a modern society. In this regard provision 279 a in the Danish Criminal Code is analyzed. In addition, the interaction between the adjacent provisions¹ and provision 279 a are analyzed, in order to clarify the extent of the penal provisions' applicability and whether or not the legal safeguard is adequate.

In 1985 the penal provision 279 a was introduced after "Straffelovrådet" published their report (no. 1032/1985), inquired by the Danish Department of Justice. The implementation of the provision regarding data fraud came despite of the Danish Prosecution Service and the Danish police questioning the necessity hereof. It came at a time where there were little digitalisation of the society and the possibility of committing digitalised criminal actions were also not common. Even so it was a sign of preparation for the future digital evolution.

Almost 30 years have passed, and the occurrence of data related crime has risen to ever new levels. Therefore, we have found it important to analyze the applicability of provision 279 a and how it differentiates from the other acquisitive crimes that has traditionally been used and have continuously been used to this day, even though the performed criminal action contains a data related aspect. Therefore, we have found it essential to look at the adjacent provisions in relation to 279 a in the Danish Criminal Code.

The purpose of analysing of the adjacent provisions is to create an overview of the applicational boundary between these and provision 279 a. We have furthermore analyzed relevant case law regarding said applicational boundary litigation. This analysis has made it possible to distinguish the practical application between provision 279 a and the traditionally used penal provisions.

The above-mentioned work has resulted in the following conclusion.

Firstly, we can conclude that the boundaries between; provision 279 a; provision 276 regarding theft and 279 regarding fraud have been made clear through precedent.

Secondly, case law on the boundaries between; provision 279 a; provision 278 regarding embezzlement; provision 280 regarding mandate fraud and provision 301 regarding skimming, continues to be unclear.

Lastly, we have decided to examen the implementation of a legal safeguard against digital acquisitive crimes in our fellow Nordic countries and the OECD. This has given us a perspective on some different approaches to this exact problem.

¹ The Danish Criminal Codes; § 276, § 278, § 279, § 280 and § 301

Indholdsfortegnelse

KAPITEL 1 – INTRODUKTION	7
1.1 - INDLEDNING	7
1.2 - PROBLEMFORMULERING	8
1.3 - METODE OG RETSKILDER	8
1.4 - AFGRÆNSNING	10
KAPITEL 2 - STRAFFELOVENS § 279 A.....	12
2.1 - TILBLIVELSEN	12
2.2 - ORDLYDEN	14
2.2.1 - Straffelovens § 279 a's første led	14
2.2.1.1 - "Ændrer, tilføjer eller sletter"	14
2.2.1.2 - "Oplysninger og programmer"	15
2.2.1.3 - "Elektronisk databehandling"	15
2.2.2 - Straffelovens § 279 a's andet led.....	16
2.2.2.1 - "I øvrigt søger at påvirke resultatet af en elektronisk databehandling"	16
2.3 - RETSSTRIDIGHEDEN	17
2.4 - FORSÆTTET	17
2.5 - FULDBYRDELSEN	18
2.6 - ANVENDELSEN I PRAKSIS	19
2.6.1 - Anvendelsen fra 1985 til 1990.....	19
2.6.2 - Anvendelsen fra 1990 til 2002.....	19
2.6.3 - Anvendelsen fra 2002 til 2015.....	20
2.6.4 - Anvendelsen fra 2015 til 2023.....	21
2.7 - DELKONKLUSION	22
KAPITEL 3 - DE TILSTØDENDE BESTEMMELSER	23
3.1 - STRAFFELOVENS § 279.....	23
3.1.1 - Retsstridig fremkaldelse	23
3.1.2 - Vildfarelse	24
3.1.3 - Påføre et formuetab	24
3.1.4 - Forsæt	25
3.1.5 - Fuldbyrkelse	25
3.2 - STRAFFELOVENS § 278, STK. 1, NR. 3	25
3.2.1 - Betroede penge	26
3.2.2 - Uretmæssigt forbrug.....	27
3.2.3 - Forsæt	27
3.2.4 - Fuldbyrkelse	27
3.3 - STRAFFELOVENS § 280.....	27
3.3.1 - Straffelovens § 280, stk. 1, nr. 1	28

3.3.2 - Straffelovens § 280, stk. 1, nr. 2	29
3.3.3 - Forsæt	30
3.3.4 - Fuldbyrkelse	30
3.4 - STRAFFELOVENS § 276.....	30
3.4.1 - Fremmed rørlig ting.....	30
3.4.2 - Økonomisk værdi	31
3.4.3 - Varetægt.....	31
3.4.4 - Forsæt	31
3.4.5 - Fuldbyrkelse	32
3.5 - STRAFFELOVENS § 301.....	32
3.5.1 - “Fremstiller, anskaffer sig, besidder, eller videregiver”	32
3.5.2 - Straffelovens § 301, stk. 1, nr. 1.....	33
3.5.3 - Straffelovens §301, stk. 1, nr. 2.....	33
3.5.4 - Forsæt	33
3.5.5 - Fuldbyrkelse	33
3.6 - DELKONKLUSION	34
KAPITEL 4 – STRAFFELOVENS § 279 A I PRAKSIS	36
4.1 - STRAFFELOVENS § 279 KONTRA § 279 A.....	36
4.1.1 - Vildfarelse	36
4.1.2 - Retspraksis.....	38
4.1.3 - Landsrettens afgørelse	39
4.1.4 - Ændring af tiltalepraksis.....	40
4.1.5 - Opsummering	41
4.2 - STRAFFELOVENS § 278, STK. 1, NR. 3 OG § 280 KONTRA § 279 A VEDRØRENDE ANSÆTTELSESFORHOLD ..	42
4.2.1 - Indledende bemærkninger	42
4.2.2 - Retspraksis vedrørende straffelovens § 279 a	43
4.2.2.1 - Uberettigede dispositioner i ansættelsesforhold	43
4.2.2.2 - Uberettigede dispositioner overfor kunder	44
4.2.2.3 - Øvrige betroelsesforhold.....	45
4.2.3 - Retspraksis vedrørende straffelovens § 278, stk. 1, nr. 3	45
4.2.3.1 - Uberettigede dispositioner i ansættelsesforhold	45
4.2.3.2 - Uberettigede dispositioner overfor borgere	46
4.2.3.3 - Øvrige betroelsesforhold.....	46
4.2.4 - Retspraksis vedrørende straffelovens § 280	46
4.2.4.1 - Uberettigede dispositioner i ansættelsesforhold	46
4.2.4.2 - Uberettigede dispositioner overfor borgere	47
4.2.4.3 - Øvrige betroelsesforhold.....	47
4.2.5 - Afgrænsningsproblematikken.....	47
4.2.6 - Opsummering	48
4.3 - STRAFFELOVENS § 276 KONTRA § 279 A.....	49

4.3.1 - Straffelovrådets bemærkninger.....	49
4.3.2 - Det forhenværende synspunkt	50
4.3.3 - Det nye synspunkt	50
4.3.4 - Retspraksis før U.2014.1688.V	51
4.3.5 - U.2014.1688.V og retspraksis herefter.....	51
4.3.6 - Usikker tiltalepraksis	53
4.3.7 - Todeling af gerningsindholdet.....	54
4.3.8 - Opsummering	55
4.4 - STRAFFELOVENS § 280 KONTRA § 279 A.....	56
4.4.1 - Opsummering	58
4.5 - STRAFFELOVENS § 301 KONTRA § 279 A.....	59
4.5.1 - Forsøg på databedrageri efter straffelovens § 279 a, jf. § 21	59
4.5.2 - Grænserne mellem straffelovens § 279 a, jf. § 21 og § 301	60
4.5.2.1 - Straf i sammenstød.....	61
4.5.3 - Retspraksis vedrørende straffelovens § 279 a, jf. § 21, og § 301	61
4.5.4 - Opsummering	63
4.6 - DELKONKLUSION	63
KAPITEL 5 – TILTALEKORREKTION	67
5.1 - ANKLAGEMYNDIGHEDENS OPGAVER	67
5.2 - DOMSTOLENES BEHANDLING	68
5.3 - BETYDNINGEN AF BERIGTIGELSE ELLER UDVIDELSE FOR TILTALTE.....	68
5.4 - DELKONKLUSION	68
KAPITEL 6 – HENSIGTSMÆSSIG ANVENDELSE?	70
6.1 - HENSIGTSMÆSSIG ANVENDELSE EFTER STRAFFELOVRÅDETS BETÆNKNING NR. 1032/1985?.....	70
6.2 - FREMRYKKET FULDBYRDELSMOMENT	70
KAPITEL 7 - PERSPEKTIVERING	72
7.1 - INDLEDENDE BEMÆRKNINGER	72
7.2 - STRAFFELOVRÅDETS BEMÆRKNINGER I BETÆNKNING NR. 1032/1985	72
7.3 - DET NORSKE STRAFFELOVRÅDS BETÆNKNING NOU 1985:31	73
7.4 - DET SVENSKKE SYNSPUNKT	75
7.5 - FINSK LØSNING AF AFGRÆNSNINGSPROBLEMATIKKEN	75
7.6 - OECD'S ANBEFALINGER OG GUIDELINES	77
7.7 - OPSUMMERING.....	77
KAPITEL 8 - KONKLUSION	79
LITTERATURLISTE.....	82
JURIDISK LITTERATUR	82
LOVGIVNING, LOVFORSLAG MM.....	83

BETÆNKNINGER.....	84
RETSPRAKSIS	85
RAPPORTER, REDEGØRELSE OG ÅRSBERETNINGER.....	86

Kapitel 1 – Introduktion

1.1 - Indledning

Ifølge Europa Kommissionens DESI² 2022, er Danmark et af de førende lande indenfor digitaliseringen af samfundet.³ Danmark har været med i toppen af listen siden 2015, hvor opgørelsen begyndte.⁴

Umiddelbart er det en god placering – vi har mulighed for at gøre næsten alt online, og vi kan let tilgå vores bank, MitID og andre vigtige personfølsomme oplysninger. Dog kan denne topplacering unægteligt skabe problemer. Ét af disse vil være, at vi gradvist bliver mere eksponeret for kriminalitet på baggrund af denne digitalisering;

“Konkret modtog politiet 7.000 anmeldelser om databedrageri i fjerde kvartal af 2022. (...) Det er en stigning på 49% i forhold til fjerde kvartal af 2021”⁵

Generelt set er databedrageri, når en eller flere gerningspersoner udnytter IT til at opnå en økonomisk gevinst.⁶

Som et eksempel på denne digitale udvikling, er den tilsyneladende igangværende afskaffelse af finansielle midler i fysisk form.⁷ Vi betaler med, overfører fra og administrerer vores økonomi fra vores smartphones. Som et resultat af dette, rykker mere og mere berigelseskriminalitet også online.

Med den digitale udvikling og vores stadigt stigende tilstedeværelse i den digitale verden, vil kriminaliteten på disse platforme naturligt også stige. Denne tendens ses desværre allerede.⁸

Med den stigende digitalisering, er det ikke utænkeligt at lignende sager i fremtiden vil finde sted. Danmark har dog, for at imødekomme denne ovenfor nævnte digitale evolution, netop fået landets første digitaliseringsminister.⁹ Her vil formålet blandt andet være at sikre en kontrolleret fremdrift af denne digitale udvikling. Dette må også være et tegn på, at digitalisering netop er kommet for at blive, og fortsat vil være en stor del af danskernes liv og det moderne samfund.

² Digital Economy and Society Index

³ <https://digital-strategy.ec.europa.eu/en/policies/desi> - The Digital Economy and Society Index (DESI) – Sidst besøgt d. 11/5 2023

⁴ <https://em.dk/media/14566/redegørelse-om-danmarks-digitale-vækst-2022.pdf> - Redegørelse om Danmarks digitale vækst 2022 – Sidst besøgt d. 11/5 2023

⁵ <https://politiken.dk/indland/art9196874/Flere-anmelder-bedrageri-til-politiet---særligt-databedrageri-fylder> - Flere anmelder bedrageri til politiet – særligt databedrageri fylder – Sidst besøgt d. 11/5 2023

⁶ <https://badv.dk/faq/hvad-er-databedrageri/> - Hvad er databedrageri? – Sidst besøgt d. 11/5 2023

⁷ <https://www.berlingske.dk/dine-penge/forskere-spaar-kontantloest-danmark-i-2025> – Forskere spår kontantløst Danmark i 2025 – Sidst besøgt d. 11/5 2023

⁸ <https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=40257> – Fortsat stigning i anmeldelser om bedrageri – Sidst besøgt d. 11/5 2023

⁹ <https://www.altinget.dk/digital/artikel/marie-bjerre-om-digital-brydningstid-mere-og-hurtigere-er-ikke-laengere-maalet-nu-handler-det-om-den-rigtige-digitalisering> - Hun er Danmarks første minister på området: Mere og hurtigere er ikke længere målet, nu handler det om den rigtige digitalisering – Sidst besøgt d. 11/5 2023

Denne udvikling vil utvivlsomt medføre en stigende udnyttelse af de samfundsnyttige digitale systemer. I den forbindelse er det mindst lige så vigtigt at have et tilstrækkeligt forsvar mod kriminalitet, der søger at udnytte det digitaliserede samfund. Det bedste, og eneste, strafferetlige værn vi har mod databedrageri, er straffelovens, herefter benævnt STRFL., § 279 a. Det er vigtigt for retssikkerheden, at der lægges større fokus på netop denne bestemmelse. For benyttes den overhovedet, i praksis, efter hensigten, og er den tilstrækkeligt dækkende på et område, der er i konstant udvikling?

1.2 - Problemformulering

Denne kandidatafhandling har til formål at undersøge den strafferetlige beskyttelse mod digital berigelseskriminalitet i det moderne samfund. I den forbindelse vil STRFL. § 279 a analyseres. Derudover vil samspillet mellem de tilstødende paragraffer og STRFL. § 279 a blive analyseret, for at belyse om det strafferetlige værn mod digital berigelseskriminalitet og databedrageri er tilstrækkeligt.

1.3 - Metode og retskilder

Den ovenfor nævnte problemformulering, vil i denne kandidatafhandling blive besvaret ved at benytte den retsdogmatiske metode, hvor gældende ret bliver beskrevet, analyseret og systematiseret.¹⁰ Som resultat af en retlig analyse af retspraksis på området omhandlende databedrageri, og de tilstødende bestemmelser, vil det være muligt at fastlægge den retlige ramme for rækkevidden af databedrageribestemmelsen i STRFL. § 279 a. Disse tilstødende bestemmelser er STRFL. § 276 om tyveri, § 278 om underslæb, § 279 om bedrageri, § 280 om mandatsvig og § 301 om skimming. Når de tilstødende bestemmelser nævnes i løbet af denne afhandling, vil det være disse netop nævnte bestemmelser der er tale om.

Retstilstanden vil blive beskrevet, ved at tage udgangspunkt i STRFL. § 279 a, og herefter de tilstødende bestemmelser. STRFL. § 279 a er ikke behandlet meget i den juridiske litteratur. Her er der primært tale om artikler samt årsberetninger fra Anklagemyndigheden, som er fra bestemmelsens indførsel i 1985. Hertil skal det nævnes, at der kun foreligger få artikler, der kritisk forholder sig til den mere end 30 år gamle forståelse af bestemmelsens anvendelsesområde. På baggrund af dette er det muligt, at fortolkningen og det generelle billede der bliver tegnet af den juridiske litteratur, ikke er tilstrækkeligt nuanceret.

På baggrund af den, på nogle punkter utilstrækkelige, juridiske litteratur, vil denne blive suppleret med en kritisk analyse af retspraksis på området. I den forbindelse vil det blive undersøgt, hvordan STRFL. § 279 a faktisk finder anvendelse, og hvordan bestemmelsens forhold til de tilstødende bestemmelser ser ud.

Igennem afhandlingen vil de anvendte domme blive kategoriseret på en sådan måde, at det forsøger at danne et overblik over bestemmelsens historiske anvendelse – helt fra indførslen af

¹⁰ Carsten Munk-Hansen, *Den juridiske løsning: Introduktion til den juridiske metode*, (København: jurist- og økonomforbundets forlag, 2017), side 14

STRFL. § 279 a i 1985 til nu i 2023. Her vil der især være fokus på at undersøge bestemmelsens rækkevidde i forhold til de tilstødende bestemmelser. Til dette formål er der udvalgt bestemte domme, som er med til at vise både forskelle og ligheder i anvendelsesområderne.

Udover retspraksis, er den primære retskilde Straffelovrådets betænkning om datakriminalitet fra 1985.¹¹ Denne betænkning er brugt til at forstå hensigten med STRFL. § 279 a. Derudover er den også anvendt til at forstå mere om rækkevidden af denne bestemmelse. Det var netop denne betænkning, der gav anledning til, at der ved lov nr. 229 af 6. juni 1985 om ændring af straffeloven, kom en bestemmelse der omhandlende databedrageri – den bestemmelse der blev til STRFL. § 279 a.

Betænkningen er informativ, idet den blandt andet indeholder Straffelovrådets tanker og overvejelser angående nødvendigheden af, og hensigten med, databedrageribestemmelsen i STRFL. § 279 a. I betænkningen fremlagde Straffelovrådet blandt andet nogle af de fortolkninger, som enten medfører eller udelukker, at diverse typer af datakriminalitet kunne behandles efter de allerede eksisterende bestemmelser. På trods af, at betænkningen er over 30 år gammel, er den stadig en af de mest dybdegående og omfattende retskilder, der behandler STRFL. § 279 a. Her er der blandt andet tale om den historiske baggrund for bestemmelsen, tankerne bag samt hvad formålet med indførslen var.

Efterfølgende vil de tilstødende bestemmelser blive gennemgået og redegjort for – ligeledes med udgangspunkt i den juridiske litteratur på området. Dette er relevant i forhold til at få fastlagt hvor og hvordan, databedrageribestemmelsen i STRFL. § 279 a er anderledes i forhold til de tilstødende bestemmelser. Derudover er formålet også at opnå kendskab til gerningsindholdet i disse tilstødende bestemmelser.

Derefter følger et afsnit omkring anvendelsen af STRFL. § 279 a i praksis. Dette afsnit er en retlig analyse af bestemmelsens anvendelse i praksis, hvor der primært vil være fokus på at afdække bestemmelsens anvendelsesområde, og hvor grænserne til de tilstødende bestemmelser, som er nævnt ovenfor, går.

Generelt for denne afhandling, er det, som tidligere nævnt den retsdogmatiske metode, der vil finde anvendelse. For at være i stand til at undersøge, hvad der er gældende ret, må alle relevante retskilder inddrages. I den forbindelse er de pågældende lovbestemmelser væsentlige. Det er dog også muligt at fortolke på disse, da lovbestemmelser sjældent er enstydige, og formålet ikke er at benytte disse til én specifik anvendelse. Netop derfor er det væsentligt at der bliver inddraget relevant retspraksis, i forbindelse med alle de ovenfor nævnte bestemmelser - både databedrageribestemmelsen i STRFL. § 279 a og de tilstødende bestemmelser. Denne retspraksis vil være i form af tidligere afsagte domme. Disse domme er,

¹¹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*

ligesom bestemmelserne, fortolkelige, men viser på samme tid en konkret anvendelse af de benyttede lovregler, i en bestemt situation.¹²

For at systematisere gældende ret, vil der blive anvendt juridisk retslitteratur og forskellige artikler om emnet. I forbindelse hermed, er det væsentligt at være opmærksom på, at juridisk litteratur ikke er en retskilde, og derfor ikke vil være bindende. Den anvendte juridiske litteratur kan dog netop bidrage til at systematisere den gældende ret, der bliver behandlet i denne afhandling.

Generelt er formålet med anvendelsen af den retsdogmatiske metode at være i stand til at skabe et overblik over retspraksis på området, og for at kunne undersøge hvordan de enkelte bestemmelsers anvendelsesområder er anvendt og fortolket af domstolene.

Derudover vil den retsdogmatiske metode ligeledes blive anvendt i afhandlingens perspektiveringsafsnit. Her vil der blive draget paralleller til nordisk ret, for at se hvordan de øvrige nordiske lande har grebet problemet med databedrageri an. I den forbindelse vil der ikke blive fremsat konkrete løsningsforslag, da dette ikke stemmer overens med den retsdogmatiske metode, som overordnet set er anvendt gennem hele afhandlingen. Brugen af den nordiske ret, er derfor udelukkende inddraget for at forsøge at danne et retvisende billede på dansk ret i forhold til vores nordiske naboer.

I forbindelse med det ovenfor nævnte perspektiveringsafsnit, er det væsentligt at holde for øje, at den anvendte metode ikke er retspolitisk. Forskellen på den retsdogmatiske metode og den retspolitiske metode er, at den retspolitiske metode omhandler, hvordan retstilstanden bør være, og ikke hvordan den er.¹³

1.4 - Afgrænsning

Formålet med dette afsnit er at afgrænse specialets problemfelt. Dette bidrager til at skabe en tydelig og fast ramme om det overordnede emne, samt er med til at definere de konkrete fokuspunkter for specialet.

Eftersom specialet omhandler digital berigelseskriminalitet, herunder nærmere bestemt databedrageri, vil det umiddelbart være relevant at behandle jurisdiktionen på dette område. Her vil det særligt være i situationer, hvor den kriminelle handling indeholder et grænseoverskridende element, hvilket vil medføre, at virkningsprincippet skal anvendes. I dette speciale vil denne problemstilling dog ikke blive behandlet, da der udelukkende fokuseres på nationale forbrydelser, og dermed territorialprincippet.

Det er yderligere valgt, at der i specialet ikke vil være fokus på strafferammen for de pågældende og anvendte bestemmelser gennem specialet. Derudover vil der ikke blive lagt

¹² Peter Blume, *Retssystemet og juridisk metode*, (København: jurist- og økonomforbundets forlag, 2016), side 55

¹³ <https://dejuridiskemetoder.digi.hansreitzel.dk/?id=222> – De juridiske metoder – Sidst besøgt d. 11/5 2023

vægt på strafferammen, når den udvalgte retspraksis løbende gennemgås og anvendes. Dette er valgt, da specialet ikke har til formål at undersøge hvorvidt strafferammen er ensartet eller passende, men derimod om de pågældende bestemmelser kontinuerligt anvendes korrekt og på de påtænkte kriminelle handlinger.

I dette speciale vil der udelukkende blive fokuseret på databedrageribestemmelsen i STRFL. § 279 a, samt de tilstødende bestemmelser. Disse pågældende bestemmelser findes i STRFL. § 276, § 278, § 279, § 280 og § 301.

STRFL. § 278 om underslæb afgrænses til udelukkende at omhandle og fokusere på stk. 1, nr. 3. Bestemmelsens stk. 1, nr. 1 og stk. 1, nr. 2 har ikke et anvendelsesområde der vil falde ind under digital berigelseskriminalitet, og vil af denne grund ikke blive behandlet dybdegående. Dette er valgt, da der i specialet fokuseres på netop digital berigelseskriminalitet.

Som tidligere nævnt omhandler dette speciale digital berigelseskriminalitet og cybercrime. I denne forbindelse er det nødvendigt at præcisere, at det der vil blive behandlet, er bestemmelser der har overlappende gerningsindhold med STRFL. § 279 a omkring databedrageri. Dette betyder, at andre bestemmelser samt retspraksis om andre former for digitale forbrydelser ikke vil blive behandlet. Dette kunne eksempelvis være bestemmelser omhandlende digitale sexkrænkelser.

I dette speciale vil der til slut være en perspektivering, hvori anden nordisk ret vil blive anvendt. Det er dog væsentligt at påpege, at denne kun bliver anvendt i perspektiveringsafsnittet, og dermed ikke vil blive behandlet i dybden eller lagt til grund for andre dele i specialet. Perspektiveringsafsnittet er lagt ind i specialet lige inden konklusionen, men vil ikke udgøre en del af konklusionen. Dette begrundes med, at perspektiveringsafsnittet ikke som udgangspunkt bidrager til besvarelsen af vores problemformulering.

Slutligt er det vigtigt at påpege, at ansvaret hos netværksejerne samt ejerne af de platforme der anvendes til at begå de kriminelle handlinger, ikke vil blive behandlet eller taget i betragtning.

Kapitel 2 - Straffelovens § 279 a

I det følgende afsnit vil anvendelsesområdet for STRFL. § 279 a, også kaldet databedrageribestemmelsen, blive belyst og behandlet ud fra den foreliggende juridiske litteratur. Her vil der blive redegjort for bestemmelsens tilblivelse, samt indhold og formål. Dette er med henblik på at opnå kendskab til bestemmelsens praktiske anvendelse, og afgrænsning til de tilstødende bestemmelser.

2.1 - Tilblivelsen

Databedrageribestemmelsen blev indsat d. 6. juni 1985 ved vedtagelsen af Lov 1985-06-06 nr. 229 om ændring af straffeloven. Bestemmelsens vedtagelse bygger på Straffelovrådets betænkning om datakriminalitet, nr.1032/1985, efter Justitsministeriet anmodede om en udtalelse, om hvorvidt de daværende straffebestemmelser udgjorde et tilstrækkeligt og tilfredsstillende strafferetligt værn mod kriminalitet, omhandlende elektronisk databehandling.¹⁴

I Justitsministeriets anmodning henviste de til en række sager der havde modtaget offentlig omtale, og givet anledning til diskussion. Alle de henviste sager var på det pågældende tidspunkt stadig under behandling hos enten politiet eller Anklagemyndigheden. Justitsministeriet oplyste dog, at Anklagemyndigheden endnu ikke havde modtaget en sag omhandlende datakriminalitet, hvor de allerede gældende straffebestemmelser ikke fandt anvendelse. Ikke desto mindre fandt Justitsministeriet det hensigtsmæssigt at udføre en vurdering af den gældende ret.¹⁵

Gennem Straffelovrådets undersøgelse af flere af bestemmelserne i straffeloven, kom de frem til den konklusion, at gældende ret på flere af bestemmelserne var tilstrækkelig. Bestemmelserne blev vurderet til også at omfatte datakriminalitet, og Straffelovrådet anså det derfor ikke nødvendigt at ændre i bestemmelsernes udformning.¹⁶

Straffelovrådet fandt dog, at en af de bestemmelser der ikke kunne anses at omfatte datakriminalitet på en tilstrækkelig og tilfredsstillende måde, var drageribestemmelsen. Derfor anbefalede Straffelovrådet, at det var nødvendigt med indførslen af den nuværende § 279 a i straffeloven. I undersøgelsen fandt Straffelovrådet netop, at der kunne forekomme tilfælde, hvor der blev indtastet uberettigede eller urigtige oplysninger i et datasystem, og hvor virksomhedens drift var af en sådan automatiseret karakter, at der ikke optrådte en person, der vildledes i databehandlingsprocessen.¹⁷

¹⁴ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 5

¹⁵ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 5

¹⁶ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 17

¹⁷ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 47

På samme måde fandt Straffelovrådet at der kunne forekomme situationer, hvor en ansat blot ville følge et datasystems anvisning og grundet sin underordnede stilling, ikke ville vurdere de angivne oplysningers validitet.¹⁸

Det var af Straffelovrådets opfattelse, at disse situationer heller ikke kunne omfattes af underslæbsbestemmelsen i STRFL. § 278, stk. 1, nr. 3, eller den subsidiære bestemmelse om mandatsvig i STRFL. § 280.¹⁹ Disse bestemmelser blev begge anvendt i praksis, særligt ved forhold hvor handlingen blev udført af en ansat, men Straffelovrådet fastslog at bestemmelserne ikke var udformet med henblik på at omfatte datakriminalitet. Af den grund kunne der forekomme situationer, hvor det fandtes mindre naturligt at anvende henholdsvis underslæbs- og mandatsvigsbestemmelsen.²⁰

Straffelovrådet foreslog, på baggrund af ovenstående argumentation og den praksis der forelå hos de andre nordiske lande²¹, at indføre en ny bestemmelse om databedrageri, der kunne omfatte alle disse bedragerilignende forhold, der faldt udenfor bedrageribestemmelsens anvendelse. Det blev foreslået, at bestemmelsen blev indsat efter bedrageribestemmelsen. På samme måde er den foreslåede udformning, udarbejdet på baggrund af bestemmelsen om almindeligt bedrageri.²²

Bestemmelsens udformning og formulering er meget bred, hvilket medfører at bestemmelsen kan forholde sig teknologineutral, og gøres relevant uanset den digitale udvikling. Dette er muligvis også en af grundene til, at det ikke har været nødvendigt at ændre bestemmelsens ordlyd, siden indførelsen i 1985. Modsat udgør det også en svaghed ved bestemmelsen, da udformningen fremsætter en ubestemmelig afgrænsning, der kan medføre en usikkerhed om hvorvidt bestemmelsen faktisk kan finde anvendelse. I praksis har dette medført, at anvendelsen af bestemmelsen er fundet besværlig.²³

Foruden den foreslåede indførsel af databedrageribestemmelsen, foreslog Straffelovrådet også at STRFL. § 280 blev ændret, således at databedrageribestemmelsen ville indgå i gruppen af bestemmelser der gik forud for mandatsvigsbestemmelsen. Dette ville ydermere gøre bestemmelsen om mandatsvig subsidiær i forhold til bestemmelsen om databedrageri.²⁴

Indførelsen af STRFL. § 279 a udelukker ikke anvendelsen af STRFL. § 279, da afgrænsningen mellem de to er relativt flydende. Derudover kan der forekomme situationer, hvor det vil være en vurderingssag, hvilken af de to bestemmelser der skal benyttes.²⁵ Modsat betyder

¹⁸ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 47

¹⁹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 49

²⁰ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 49-50

²¹ Dette vil blive behandlet yderligere i afhandlingens perspektivering i kapitel 7

²² Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 49 og Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 2

²³ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 2

²⁴ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 77 og 83

²⁵ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 2

indførelsen af databedrageribestemmelsen i STRFL. § 279 a, at der kan forekomme situationer omhandlende datakriminalitet hvor anvendelsen af STRFL. § 280 er uhensigtsmæssig.²⁶

Justitsministeriet anførte i sit lovforslag om ændring af straffeloven, at den tiltrådte Straffelovrådets vurdering, og udtrykte at den så det hensigtsmæssigt at fastslå, at brugen af datateknik for at skaffe sig selv eller andre uberettiget vinding, ville blive anset som en strafbar handling.²⁷

Bestemmelsens daværende, og nuværende, formulering er således;

*“For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling.”*²⁸

2.2 - Ordlyden

Som ovenfor anført, omhandlede en del af Straffelovrådets overvejelser bestemmelsens rækkevidde og nødvendighed, set i forhold til de tilstødende bestemmelser. I det kommende afsnit vil ordlyden af STRFL. § 279 a, samt de væsentlige betingelser der skal være opfyldt, før bestemmelsen kan finde anvendelse, blive analyseret.

Bestemmelsen er udformet præcis som Straffelovrådet oprindeligt formulerede den i betænkningen. Formuleringen af bestemmelsen er bygget op om bestemmelsen om almindeligt bedrageri, dog med udeladelsen af vildfarelseskravet.²⁹

Bestemmelsen er opdelt i to led, der hver vil blive behandlet særskilt i de nedenstående afsnit.

2.2.1 - Straffelovens § 279 a's første led

Bestemmelsens første led, søger at kriminalisere en retsstridig ændring, tilføjelse eller sletning af oplysninger eller programmer til elektronisk databehandling.³⁰ Netop dette indhold vil blive behandlet i det følgende.

2.2.1.1 - “Ændrer, tilføjer eller sletter”

Straffelovrådet udtrykker i betænkningen, at ordet “ændrer” i de fleste tilfælde, vil medføre en tilstrækkelig dækning af de fleste forhold der ønskes kriminaliseret ved bestemmelsens indførsel. Dog mente Straffelovrådet, at tilføjelsen af udtrykkene “tilføjer” og “sletter”, burde være til stede i formuleringen for klarhedens skyld, og for at tydeliggøre bestemmelsens fortolkning.³¹

²⁶ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 83

²⁷ LFF.1985-04-24, nr. 221

²⁸ Straffelovens § 279 a

²⁹ LFF.1985-04-24, nr. 221 og Lars Bo Langsted og Peter Helbo Langsted, *Hovedlinjer i erhvervsstrafferetten*, (København: DJØF forlag, 2020), side 107

³⁰ Straffelovens § 279 a

³¹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 80

Derudover foreligger der intet krav til hvordan, eller med hvilken metode, ændringen, tilføjes eller sletningen foretages. Det må dog antages, at der foreligger en betingelse om at den kriminaliserede handling skal have en nærhed til databehandlingen.³²

Straffelovrådet udtrykker i betænkningen, at metoden for databedrageriet både kan udføres ved hjælp af et data-teknisk apparat, som eksempelvis en dataterminal, men at det også kan være i form af den fysiske ødelæggelse af de elektroniske komponenter, for at medføre en sletning af data. Her vil forholdet adskille sig fra hærværksbestemmelsen i STRFL. § 291, ved at der forelægger et berigelsesforsæt.³³ Denne bestemmelse i STRFL. § 291 omhandlende hærværk, vil ikke blive behandlet yderligere i denne afhandling.

2.2.1.2 - "Oplysninger og programmer"

Ifølge bestemmelsens formulering skal ændringen, tilføjes eller sletningen udføres mod *"oplysninger eller programmer"*. Definitionen af disse begreber er der ikke redegjort for i betænkningen, og der foreligger derfor ikke nogen beskrivelse af, hvad disse begreber mere præcist egentlig dækker over.

Straffelovrådet udtrykker i betænkningen, at et datasystem består af fire centrale elementer;

- "1) den centrale enhed, der udfører den angivne databehandling på baggrund af de tilgængelige oplysninger og programmer,*
- 2) terminalen, der anvendes til at indtaste oplysninger til dataanlægget,*
- 3) transmissionsforbindelsen, der forbinder den centrale enhed med en dataterminal, og*
- 4) de lagrede oplysninger og programmer, der anvendes af det centrale system, til at udføre den anmodede databehandling."*³⁴

Dog fastslår Straffelovrådet i betænkningen, at det er uden betydning hvorvidt oplysningerne eller programmet er lagret i et datasystem, eller om den omhandlende data er under transmission mellem to datasystemer.³⁵

2.2.1.3 - "Elektronisk databehandling"

På samme måde som begreberne *"programmer og oplysninger"*, som netop er behandlet ovenfor, er definitionen på *"elektronisk databehandling"* ligeledes ikke præcist oplyst i Straffelovrådets betænkning. Det er dog en forudsætning, at databehandlingen omfatter brugen af et dataanlæg, der anvender et datasystem.³⁶

³² Lars Bo Langsted og Peter Helbo Langsted, *Hovedlinjer i erhvervsstrafferetten*, (København: DJØF forlag, 2020), side 108 og Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 693

³³ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 81

³⁴ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 13

³⁵ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 81

³⁶ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022) side 693

Straffelovrådet udtrykker i betænkningen, at udtryk som “*data*” og “*databehandling*” sprogligt vil omfatte enhver oplysning eller behandling af oplysninger, herunder en mulig manuel behandling af oplysninger.³⁷

Denne formulering svarer dog ikke på spørgsmålet, angående hvad begrebet “*elektronisk databehandling*” dækker over. Af den grund må svaret derfor søges i den gældende retspraksis. En specifik afgrænsning af definitionen på en elektronisk databehandling, er endnu ikke blevet afgjort ved domstolene, og en mulig definition må derfor observeres gennem de eksempler der fastlægges af retspraksis.

Et af disse eksempler er Vestre Landsrets dom fra 2014, hvor fire gerningspersoner blev dømt for overtrædelse af databedrageribestemmelsen i STRFL. § 279 a. Gerningspersonerne havde oprettet en aftale hos Nets, om levering af betalingskortterminaler ved oprettelse af flere virksomheder, hvorefter gerningspersonerne brugte stjålne betalingskort³⁸ til at overføre store summe penge til egne konti. Efterfølgende videreførte de pengene til forskellige andre konti, og dele af summen blev brugt på køb af guld. Her fastslog Vestre Landsret, at en uberettiget brug af betalingskort og en terminal til hævnning, skal anses for en påvirkning af en elektronisk databehandling.³⁹

2.2.2 - Straffelovens § 279 a's andet led

Bestemmelsens andet led, søger at kriminalisere indgreb, der i øvrigt retsstridigt søger at påvirke resultatet af en elektronisk databehandling.⁴⁰ Dette indhold vil blive behandlet i det følgende.

2.2.2.1 - “I øvrigt søger at påvirke resultatet af en elektronisk databehandling”

I bestemmelsens andet led, ses en mere generel og udefineret udvidelse af bestemmelsens første led. Denne del fungerer som et tillæg, i de tilfælde hvor gerningsindholdet ikke kan falde ind under bestemmelsens første led.⁴¹

Spørgsmålet om hvorvidt der er sket en elektronisk databehandling, hvor et resultat er blevet påvirket ved selve indtastningen af data, eller først på et senere tidspunkt, skal der ikke tages stilling til i bestemmelsens andet led.⁴²

Et eksempel på et tilfælde, som ikke vil være omfattet af bestemmelsens første led, er det forhold, hvor gerningspersonen i stedet for at gribe ind i den elektroniske databehandling, ændrer de oplysninger, som senere skal indtastes af en person, med henblik på elektronisk

³⁷ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 13

³⁸ Gennem afhandlingen vil der blive anvendt flere forskellige betegnelser for et kort. Dette kan blandt andet være dankort, hævekort, betalingskort mv.

³⁹ U.2014.1688.V

⁴⁰ Straffelovens § 279 a

⁴¹ Gorm Toftegaard Nielsen, Thomas Elholm og Morten Niels Jakobsen, *Kommenteret straffelov – Speciel del*, (København: jurist- og økonomforbundets forlag, 2017), side 620

⁴² Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 82

databehandling.⁴³ I et sådan tilfælde er det ikke gerningspersonen selv, der foretager ændringen i den elektroniske databehandling. Af den grund kan gerningspersonen ikke styre, på hvilket tidspunkt den reelle ændring foretages. Vedkommende, der alt andet lige handler ud fra forudsætningen om, at de pågældende oplysninger er korrekte, kan dog blive bragt i vildfarelse. Denne vildfarelse kan i nogle tilfælde bringe situationen ind under bedrageribestemmelsen i STRFL. § 279 i stedet for STRFL. § 279 a, andet led.⁴⁴ Netop denne situation, vil blive undersøgt nærmere i afsnit 4.1.

Generelt for STRFL. § 279 a er, at anklageskriftet sjældent fastlægger, hvorvidt den pågældende forbrydelse er en handling der overtræder bestemmelsens første eller andet led. Derudover bemærkes det, at bestemmelsens første led oftere finder anvendelse end andet led.⁴⁵

2.3 - Retsstridigheden

I både første og andet led i databedrageribestemmelsen, findes der et krav om, at det pågældende forhold skal være retsstridigt. Dette omfatter både den intetanende person og den ansattes unormale fremgangsmåde.⁴⁶ Kravet om retsstridighed bevirker, at der ikke må foreligge en objektiv straffrihedsgrund, som eksempelvis samtykke.⁴⁷

For at forklare dette, kan der blandt andet kigges på en dom fra 2017.⁴⁸ Her ville forsvareren overbevise retten om, at den tiltalte, efter ønske fra den forurettede, havde overført 600.000 kroner fra den forurettedes konto til sin egen. Det var dog ikke muligt at overbevise retten om dette. I en sådan situation er det væsentligt at kigge på netop vurderingen af, om der foreligger samtykke. Var det bevist, at de pågældende overførsler var sket på baggrund af den forurettedes ønske herom, ville der dermed ikke være tale om en retsstridig handling, da den tiltalte foretog overførslen. Her vil det altså være spørgsmålet om hvorvidt der forelå samtykke eller ej, forud for overførslen, der ender med at afgøre hvorvidt databedrageribestemmelsen i STRFL. § 279 a kan finde anvendelse.

2.4 - Forsættet

Efter STRFL. § 19 modsætningsvist, kræver strafansvar efter databedrageribestemmelsen forsæt. Da der er tale om berigelsesforbrydelser i STRFL. § 279 a, er der et krav om berigelsesforsæt hos gerningspersonen.⁴⁹ Dette betyder, at gerningspersonen ved den kriminelle handling søger at opnå en uberettiget vinding, der enten kommer vedkommende selv eller en tredjemand til gode.

⁴³ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 81

⁴⁴ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 81

⁴⁵ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 161

⁴⁶ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 162

⁴⁷ Knud Waaben, *Strafferettens almindelige del I – Ansvarslæren*, (København: Karnov Group, 2015), side 64

⁴⁸ TfK.2017.1158/2.Ø

⁴⁹ <https://denstoredanske.lex.dk/berigelsesforbrydelser> - Berigelsesforbrydelser - Sidst besøgt d. 11/5 2023

Ordlyden af databedrageribestemmelsen, indeholder ikke et krav om, at handlingen skal føre til et formuetab hos den forurettede, før gerningen er fuldbyrdet.⁵⁰ Det vil sige, at databedrageribestemmelsens gerningsindhold fuldbyrdes tidligere end det eksempelvis er tilfældet i STRFL. § 279, som omhandler almindeligt bedrageri. Hvornår der sker fuldbyrdelse i STRFL. § 279 a, vil blive beskrevet nærmere i det følgende.

2.5 - Fuldbyrdelsen

STRFL. § 279 a fuldbyrdes tidligere end de øvrige berigelsesforbrydelser. Her sker fuldbyrdelsen ved gerningspersonens disposition og altså ikke først, når vedkommende har opnået en uberettiget vinding. Dette kaldes fremrykket fuldbyrdelsesmoment. Selve fuldbyrdelsesmomentet er det tidspunkt, hvor den pågældende forbrydelse anses for at være fuldbyrdet.⁵¹ Det vil sige, at fuldbyrdelsesmomentet er når forsøget afsluttes, og den kriminelle gerning er gennemført eller realiseret.⁵²

I databedrageribestemmelsen betyder det, at indholdet af første led er realiseret, når gerningspersonen med berigelsesforsæt ændrer, tilføjer eller sletter oplysninger eller programmer⁵³, og gerningspersonen kan opnå en vinding uden at foretage sig yderligere.⁵⁴ I denne sammenhæng bemærkes det i øvrigt, at databedrageribestemmelsen anses for værende fuldbyrdet, ligegyldigt om gerningspersonen rent faktisk opnår den tiltænkte, og uberettigede, vinding eller ej.

Andet led i STRFL. § 279 a er realiseret, når der er foretaget en anderledes handling end hvad der fremgår af bestemmelsens første led, hvor der er et berigelsesforsæt samt et forsæt til at søge at påvirke resultatet af en databehandling.⁵⁵ ⁵⁶ I denne forbindelse er det ligegyldigt, at et eventuelt tab først realiseres hos den forurettede på et senere tidspunkt.

Det har været Straffelovrådets opfattelse, at det var nødvendigt at fuldbyrdelsen i databedrageribestemmelsen faldt på et tidligere tidspunkt, end det eksempelvis er tilfældet i nogle af de tilstødende bestemmelser.⁵⁷ Dette blev begrundet med, at der potentielt kunne opstå tilfælde, hvor det ville være umuligt at finde frem til oplysninger om hvornår den ulovlige databehandling havde fundet sted.⁵⁸ Netop dette er interessant at undersøge i forhold til de mere moderne muligheder, der er kommet til siden 1985. Senere i afhandlingen vil dette blive vurderet, i forhold til om indholdet af databedrageribestemmelsen fortsat er tilstrækkeligt i dag.

⁵⁰ Gorm Toftegaard Nielsen, Thomas Elholm og Morten Niels Jakobsen, *Kommenteret straffelov – Speciel del*, (København: jurist- og økonomforbundets forlag, 2017), side 620

⁵¹ Gorm Toftegaard Nielsen, *Om at lære strafferet og/eller begreber*, U.1990B.329, side 333

⁵² Gorm Toftegaard Nielsen, *Om at lære strafferet og/eller begreber*, U.1990B.329, side 334

⁵³ Straffelovens § 279 a, første led

⁵⁴ Gorm Toftegaard Nielsen, Thomas Elholm og Morten Niels Jakobsen, *Kommenteret straffelov – Speciel del*, (København: jurist- og økonomforbundets forlag, 2017), side 620

⁵⁵ Straffelovens § 279 a, andet led

⁵⁶ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 82

⁵⁷ Eksempelvis bedrageri

⁵⁸ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 82

2.6 - Anvendelsen i praksis

Efter den ovenstående gennemgang af databedrageribestemmelsen i STRFL. § 279 a, vil det i den forbindelse være naturligt at undersøge bestemmelsens historiske anvendelsesområde i praksis. Dette vil blive gjort med henblik på at skabe et overblik over bestemmelsens store anvendelsesområde, og for at beskrive de mulige problematikker, som vil blive behandlet senere i afhandlingen. En anden grund til at netop dette afsnit er interessant, er at bestemmelsens ordlyd, som tidligere nævnt, ikke er blevet ændret siden indførelsen i 1985. I tiden herefter er der sket en markant udvikling af det moderne og digitale samfund, som umiddelbart havde været svær at forudsige i 1985.

De følgende afsnit med relevant retspraksis, er delt op i tidsmæssige perioder. Dette er valgt, da der i begyndelsen eller slutningen af hver af perioderne er sket noget nyt i forbindelse med databedrageri. I 1990 udkom Anklagemyndighedens Årsberetning, i 2002 udgav Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet delbetænkning nr. VIII og i 2014 fastslog retspraksis afgrænsningen mellem tyveri i STRFL. § 276 og databedrageri i STRFL. § 279 a.

2.6.1 - Anvendelsen fra 1985 til 1990

Da STRFL. § 279 a blev indført, var denne bestemmelse den mest brugte bestemmelse, når det omhandlede “edb-berigelseskriminalitet”.⁵⁹ Her var der tale om sager omhandlende datakriminalitet med berigelsesforsæt.

I perioden efter bestemmelsens indførsel, fandtes det, at sager der tidligere omhandlede mandatsvig og underslæb, nu blev erstattet af sager der handlede om databedrageri. Efter bestemmelsen blev indført, omhandlede de klassiske eksempler på databedrageri ansatte der arbejdede i underordnede stillinger, som udnyttede de tilgængelige it-faciliteter, til at opnå økonomisk gevinst.⁶⁰

I en sag fra 1989 blev en bankassistent dømt for databedrageri, da vedkommende både havde brugt bankkunders konti til at betale sine egne regninger samt at flytte pengebeløb fra kunders konti til sin egen konto.⁶¹

2.6.2 - Anvendelsen fra 1990 til 2002

I denne periode begyndte nye former for digital kriminalitet at opstå. Her opstod blandt andet spørgsmålet om, hvorledes misbrug af dankort skulle behandles retligt korrekt.

Efter Anklagemyndighedens Årsberetning fra 1990, skulle misbrug af eget dankort, uanset fremgangsmåde, som hovedregel straffes som mandatsvig efter STRFL. § 280.⁶² Derudover fremgik det, at misbrug af en anden persons dankort, som udgangspunkt skulle straffes som tyveri. Afhængigt af fremgangsmåden, kunne det også være røveri eller ulovlig omgang med

⁵⁹ Anklagemyndighedens årsberetning, (1989), side 41

⁶⁰ Anklagemyndighedens årsberetning, (1989), side 51

⁶¹ U.1989.708

⁶² Anklagemyndighedens årsberetning, (1990), side 108

hittegods. Den efterfølgende brug af det pågældende dankort med den rette kode, skulle ligeledes dømmes som tyveri efter STRFL. § 276.⁶³

Retspraksis i sager om tyveri af dankort samt uberettigede hævnninger, viser at der i denne periode rejses tiltale i overensstemmelse med Anklagemyndighedens retningslinjer. Et eksempel herpå er fra 2001, hvor den tiltalte blev dømt for tyveri, da vedkommende havde tilegnet sig en anden persons dankort, og efterfølgende foretaget uberettigede hævnninger på kortet.⁶⁴

Derudover viser praksis også, at både Anklagemyndigheden og domstolene skulle tage stilling til, hvorledes brugen af falske dankort retligt skulle vurderes, da denne situation ikke var behandlet i Anklagemyndighedens Årsberetninger. I praksis blev dette dømt som værende databedrageri. Eksempelvis er der en dom fra 2000, hvor de tiltalte blev dømt for databedrageri, da de havde foretaget hævnninger med forfalskede hævekort. De pågældende gerningspersoner havde aflæst kortoplysninger på over 100 betalingskort, hvorefter de fremstillede forfalskede hævekort.⁶⁵

Et specielt eksempel, der også viser bestemmelsens brede anvendelsesområde, er en anden dom fra 2000. Her blev den tiltalte dømt efter databedrageribestemmelsen, da vedkommende tilføjede et ekstra kredsløb på sin egen mobiltelefon. På denne måde kunne den tiltalte hacke sig ind på en anden persons mobiltelefon, for derefter at have samtaler fra sin egen mobiltelefon, igennem den anden persons mobiltelefon. Ved denne fremgangsmåde, blev regningen for den tiltaltes opkald sendt til den person, der ejede den anden mobiltelefon.⁶⁶

2.6.3 - Anvendelsen fra 2002 til 2015

Denne periode bar præg af, at Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet udgav delbetænkning nr. VIII i 2002. I denne blev det især overvejet, hvorvidt der var anledning til ændringer, i forhold til kriminalitet med betalingskort. I den forbindelse blev der indført en bestemmelse, der kriminaliserede uberettiget besiddelse mv. af betalingsinformationer.⁶⁷ Bestemmelsen blev til STRFL. § 301, som bliver behandlet nærmere i afsnit 3.5.

I 2005 beskrev Mads Bryde Andersen det klassiske eksempel på databedrageri. Det blev fremstillet som en situation, hvor gerningspersonen ved at trænge ind i et system til kontoførelse, retsstridigt overfører beløb til sin egen konto, som efterfølgende hæves.⁶⁸

Et andet fokus var i perioden fra 2002 til 2015, på at klarlægge, hvorledes brug af andres dankort og koder skulle dømmes. Særligt én bestemt situation, gav i praksis anledning til

⁶³ Anklagemyndighedens årsberetning, (1990), side 110

⁶⁴ U.2001.1980/2.Ø

⁶⁵ U.2000.1881/1.Ø

⁶⁶ Tfk.2000.93

⁶⁷ Betænkning nr. 1417, (København 2002), *Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet*, side 152

⁶⁸ Mads Bryde Andersen, *IT-retten*, (København: Gjellerup, 2005) side 741

besvær.⁶⁹ Her var der tale om hændelser, hvor gerningspersonen stjal et betalingskort og derefter brugte kortet i en hæveautomat, til at lave kontante hævninger. Frem til 2014 blev sådanne sager dømt efter STRFL. § 276, som er tyveribestemmelsen. Efter 2014 blev de dømt efter STRFL. § 279 a. Dette behandles nærmere i afsnit 4.3.

2.6.4 - Anvendelsen fra 2015 til 2023

I den seneste periode er der kommet mange nye former for databedrageri. Gerningspersonerne har i nogle tilfælde været nødt til at være mere kreative i praktiseringen af deres kriminelle handlinger. I denne periode er der blandt andet faldet dom over medarbejdere, der har snydt deres arbejdsplads for mange millioner af kroner, og flere tilfælde, hvor STRFL. § 279 a har været brugt i sager hvor ældre personer er blevet scammed.

En af de nyere former for kriminalitet, er en blanding af tricktyveri og databedrageri. Her ses der i praksis fra denne periode, at det især er unge mennesker der bedrager ældre. I starten af 2022 blev en 22-årig mand idømt fængsel i 1 år og 3 måneder for netop dette. I denne situation, havde gerningspersonen, sammen med flere gerningspersoner, ringet til ældre kvinder, og udgivet sig for at være fra kvindernes bank. De fortalte kvinderne, at deres hævekort var ved at blive misbrugt, og at der ville komme en medarbejder fra banken og afhente kortene. I forbindelse dermed, blev kvinderne bedt om at udlevere koden til hævekortene. Derefter blev der hævet kontanter og kortene blev brugt til at købe varer i butikker.⁷⁰

En anden dom i denne periode var fra 2022, der ligeledes omhandlede svindel og databedrageri. Her var der tale om brug af overvågningsudstyret kaldet "keylogger", der blev sat på tastaturer på biblioteker over hele landet. Herved skaffede gerningspersonerne sig adgang til brugernavne og adgangskoder til NemID, og efterfølgende stjal gerningspersonerne nøglekortene fra de forurettedes postkasser. Efterfølgende blev der overført penge fra de forurettedes konti til gerningspersonernes konti, ligesom der blev optaget lån og købt varer. Der var tale om formuetab, eller risiko herfor, for over 45 mio. kroner. Der blev ved dommen lagt vægt på, at databedragerierne var sket i forening med andre, som en del af en organisation med et fast hierarki, herunder med en klar koordinering og fordeling af opgaverne.⁷¹

Som tidligere nævnt, er der i denne periode faldet dom i en række sager, hvor ansatte er fundet skyldige i databedrageri, i deres arbejdsstillinger. I en sag fra 2022, blev en af virksomhedens sælgere dømt efter STRFL. § 279 a. I denne situation bestod databedrageriet i, at gerningspersonen havde lagt fiktive ordrer ind i virksomhedens IT-system, hvorefter godtroende og intetanende lagermedarbejdere pakkede og sendt de pågældende fiktive ordrer

⁶⁹ U.2017.3056.V, TfK.2016.939.V og AM.2011.01.20B4

⁷⁰ <https://politi.dk/sydoestjyllands-politi/nyhedsliste/22-aarig-mand-doemt-for-tricktyveri-og-databedrageri-af-aeldre-kvinder/2022/01/14> - 22-årig mand dømt for tricktyveri og databedrageri af ældre kvinder – Sidst besøgt d. 11/5 2023

⁷¹ <https://www.domstol.dk/vestrelandsret/aktuelt/2022/12/3-8-aars-faengsel-for-saerlig-grove-databedragerier-ved-nemid-svindel/> - 3-8 års fængsel for særlig grove databedragerier ved NemID-svindel – Sidst besøgt d. 11/5 2023

ud. Herefter opkrævede og modtog gerningspersonen selv betaling for varerne. Dette var til et samlet beløb på ca. 5,5 mio. kroner.⁷²

En mulig forklaring på disse nye former for databedrageri, kan være at borgerne alle er blevet mere opmærksomme på netop databedrageri og snyd. Der bliver i højere grad advaret imod at give sine oplysninger til fremmede folk og virksomheder, man ikke stoler på. I denne forbindelse har politiet også oprettet en ny digital enhed, kaldet Politiets Online Patrulje (POP), der blandt andet skal forebygge sådanne situationer.⁷³

2.7 - Delkonklusion

Som det netop er gennemgået, så har anvendelsesområdet for STRFL. § 279 a ændret sig en del, fra bestemmelsens indførelse i 1985 og frem til 2023. Grundet bestemmelsens ordlyd, har denne et meget bredt anvendelsesområde, og finder som udgangspunkt anvendelse, når der er tale om en uberettiget vinding, der skaffes ved misbrug af især it-systemer. Det ses også, at brugen af bestemmelsen stadig udvikler sig, og følger med udviklingen i samfundet og i de kriminelle handlinger.

Dog er der stadig en række situationer, hvor der i praksis er nogle afgrænsningsproblemer. Her er der tale om, at STRFL. § 279 a potentielt finder anvendelse, men hvor en af de tilstødende bestemmelser på samme vis også vil være egnet til at rumme gerningsindholdet.

Videre i denne afhandling, vil netop denne problemstilling blive analyseret og vurderet.

⁷² TfK.2022.462.Ø

⁷³ <https://www.justitsministeriet.dk/wp-content/uploads/2021/08/Aftale-om-politiets-og-anklagemyndighedens-oekonomi-2021-2023.pdf> - Aftale om politiets og anklagemyndighedens økonomi 2021-2023 – Sidst besøgt d. 11/5 2023

Kapitel 3 - De tilstødende bestemmelser

Ved lov nr. 229 af 6. juni 1985 blev STRFL. § 279 a, som tidligere nævnt, indført i straffeloven. Ved indførelsen blev det gjort klart, at der ikke fandtes nogen straffebestemmelse der indeholdt dataelementet, hvorfor der potentielt kunne blive behov for en udvidet fortolkning af de eksisterende paragraffer, hvis ikke STRFL. § 279 a indførtes. En sådan udvidet fortolkning ville kunne føre til et problematisk retssikkerhedsforhold. Af denne grund var det vigtigt at få indført STRFL. § 279 a.

I det følgende afsnit vil der, kort blive redegjort for ordlyden af de tilstødende bestemmelser. Denne ordlydsfortolkning foretages med henblik på at skabe en forståelse af afgrænsningen mellem STRFL. § 279 a og de tilstødende bestemmelser. Dette er fundet væsentligt, idet de tilstødende bestemmelsers gerningsindhold i flere tilfælde kan dække kriminaliserede handlinger, der også kan falde under de tilstødende bestemmelser, hvis det ikke var for dataelementet i STRFL. § 279 a.

De tilstødende bestemmelser som bliver behandlet i denne afhandling, er som tidligere nævnt STRFL. § 276, § 278, stk. 1, nr. 3, § 279, § 280 og § 301. Disse bestemmelser vil blive behandlet i en rækkefølge, hvorefter de der har de største afgrænsningsmæssige berøringsflader behandles først.

3.1 - Straffelovens § 279

Herunder vil der følge en ordlydsfortolkning af bedrageribestemmelsen i STRFL. § 279. Det fremgår, at STRFL. § 279 lægger til grund for skabelsen af § 279 a, som det ses af straffelovrådets betænkning om datakriminalitet fra 1985. Af denne grund vil det være fundamentalt at foretage en ordlydsfortolkning af STRFL. § 279. Denne foretages, for at skabe en forståelse for gerningsindholdet i STRFL. § 279. En nærmere afgrænsning mellem netop STRFL. § 279 og STRFL. § 279 a, vil blive foretaget i afhandlingens afsnit 4.1.

Herunder vil der følge en ordlydsfortolkning, for nedenstående ordlyd af bedrageribestemmelsen i STRFL. § 279;

“For bedrageri straffes den, som, for derigennem af skaffe sig eller andre uberettiget vinding, ved retsstridigt at fremkalde, bestyrke eller udnytte en vildfarelse bestemmer en anden til en handling eller undladelse, hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab.”⁷⁴

3.1.1 - Retsstridig fremkaldelse

Som det ses i ordlyden ovenfor, er retsstridighedsbetingelsen i STRFL. § 279 det første kriterie for overtrædelse i bedrageribestemmelsen. Dette krav sikrer at domstolene har mulighed for at tage stilling til hvorvidt det konkrete tilfælde vil høre under en retsstridig handling.

⁷⁴ LBKG 2022-09-28, nr. 1360, Straffeloven

Der vil forefindes tilfælde hvori man vil opfylde alle kriterier i STRFL. § 279, dog uden at kunne fyldestgøre retsstridighedskravet.⁷⁵ Et eksempel på dette kan blandt andet være overdreven anprisning af varer.⁷⁶ Det ville eksempelvis være helt legalt at man i en annonce for en bil vil sige, at dette er verdens bedste bil, da en sådan formulering må kunne anses af køberen som værende en overdreven anprisning.

Kravet om retsstridighed findes at have en dobbelt funktion. Det henviser først og fremmest til de objektive straffrihedsgrunde. Dernæst henviser det til, at strafansvar kan være udelukket ved fortolkning, når en handling ikke burde være strafbar, til trods for at den i øvrigt opfylder de i gerningsbeskrivelsen opstillede krav.⁷⁷

3.1.2 - Vildfarelse

Den altovervejende betingelse for at benytte bedrageribestemmelsen i STRFL. § 279, er at der hos den forurettede skal foreligge en vildfarelse. En vildfarelse kan også finde sted selvom den forurettede besidder en vis skepsis overfor gerningspersonens oplysninger. Dog kan der ikke være tale om fuldbyrdelse af bestemmelsen, hvis der er tale om en meget stor mistillid.⁷⁸ Dette betyder at man ikke kan tale om en vildfarelse hvis den forurettede udviser en meget stor mistillid til gerningspersonen, forud for vildfarelsen.

Vildfarelsen skal ikke nødvendigvis være rettet mod en enkelt person, men derimod kan den være rettet mod en ubestemt kreds af personer, eksempelvis ved hjælp af en avisannonce, jf. TfK.2016.1191/2. I denne dom var der tale om at to tiltalte, der ved forudgående aftale havde indrykket en avisannonce, hvor deres virksomhed tilbød snerydning i hele Danmark, ikke havde hverken vilje eller evne til at opfylde de indgåede aftaler.⁷⁹

Vildfarelsen skal være fremkaldt, bestyrket eller udnyttet af gerningspersonen. Dette kan finde sted ved at give positivt urigtige oplysninger, men kan ligeledes finde sted ved en fortielse. Eksempelvis kan der være tale om en fortielse angående gerningspersonens dårlige økonomiske situation, ved en låne-samtale med banken.⁸⁰ Det er ligeledes et krav, at der er årsagssammenhæng mellem gerningspersonens adfærd og dispositionen.⁸¹

3.1.3 - Påføre et formuetab

Den tredje betingelse for overtrædelse af bedrageribestemmelsen er at gerningspersonen i sammenfald med fremkaldelsen, bestyrkelsen eller udnyttelsen af den forurettedes vildfarelse,

⁷⁵ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 689

⁷⁶ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 153

⁷⁷ Knud Waaben, *Strafferettens almindelig del*, (København: Karnov Group, 2015), side 66 f

⁷⁸ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 683

⁷⁹ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 683

⁸⁰ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 684

⁸¹ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 685

skal have bestemt vedkommende en tabsvoldende disposition. Dette betyder, at der skal foreligge en årsagssammenhæng mellem gerningspersonens adfærd, vildfarelsen og dispositionen.⁸² Gerningspersonens adfærd skal således foreligge inden, eller senest samtidig med, den forurettedes disposition.⁸³

Den tabsvoldende disposition består typisk i en handling, men kan som nævnt ovenfor også bestå i en undladelse.⁸⁴

Formuetab kan bestå af enten en formindskelse af aktiver eller en forøgelse af passiver. Et formuetab fortolkes bredt til også at indebære en væsentlig risiko for tab. Som eksempel herpå er dommen TfK.2008.647.Ø, hvor det var forsøgt at få en fond til at tilbagekøbe nogle anparter, og i denne proces fortiede værdien af disse for at forsøge at opnå en større gevinst, og dermed påføre fonden en risiko for et større tab.⁸⁵

3.1.4 - Forsæt

Det er et subjektivt krav, at der handles med forsæt til alle dele af gerningsindholdet i STRFL. § 279.⁸⁶ Herudover kræves det, at gerningspersonen har et berigelsesforsæt - dette ses dog hos domstolene ikke som et generelt krav. Her ses det, at det findes tilstrækkeligt at gerningspersonen har set det som sandsynligt, at der vil forekomme en vinding og et tab som følge af den kriminelle handling.⁸⁷ Knud Waaben påpeger herefter, at det vil være nærliggende at antage, at når det gælder vinding og tab, vil dette risikoforsæt træde i stedet for sandsynlighedsforsættet og dolus eventualis.

3.1.5 - Fuldbyrkelse

Fuldbyrdelsesmomentet finder sted når et formuetab, eller risiko herfor, er indtrådt.⁸⁸ Altså vil det være tilstrækkeligt, at gerningspersonen har indset at vedkommendes handling, vil kunne skabe en risiko for formuetab hos den forurettede.

3.2 - Straffelovens § 278, stk. 1, nr. 3

Herunder vil der foretages en ordlydsfortolkning af STRFL. § 278, stk. 1, nr. 3. Der fokuseres på bestemmelsens stk. 1, nr. 3, da pengeunderslæb er den del af straffebestemmelsen der findes at være en afgrænsningsproblematik med, i forhold til STRFL. § 279 a.⁸⁹

⁸² Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 684

⁸³ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 685

⁸⁴ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 685

⁸⁵ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 686

⁸⁶ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 690

⁸⁷ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 113 f

⁸⁸ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 691

⁸⁹ Nærmere beskrivelse af denne begrænsning findes i afgrænsningsafsnittet

Ordlydsfortolkningen af STRFL. § 278, stk. 1, nr. 3 er relevant, idet der i retspraksis har været afgrænsningsproblemer, i forbindelse med hvilken bestemmelse der skal benyttes. En nærmere afgrænsning mellem STRFL. § 279 a og § 278, stk. 1, nr. 3 behandles i afhandlingens afsnit 4.2.

Det er følgende ordlyd, der herunder vil blive behandlet. Som tidligere nævnt, er det dog kun stk. 1 nr. 3 der vil blive behandlet;

”For underslæb straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding

1) tilegner sig en fremmed rørlig ting, der er i hans varetægt, uden at forholdet falder ind under § 277,

2) fragår modtagelsen af pengelån eller andet lån til eje eller af en ydelse, for hvilken der skal svares vederlag,

3) uretmæssig forbruger ham betroede penge, selv om han ikke var forpligtet til at holde disse afsondrede fra sin egen formue”⁹⁰

3.2.1 - Betroede penge

I kontrast til STRFL. § 278, stk. 1, nr. 1, kan genstanden for underslæb her være fuldstændig i gerningspersonens ejendomsret. Der findes ingen pligt til at afsondre disse midler fra sin egen formue - dog kan det fremgå af en underliggende aftale.

Bestemmelsen omhandler kun penge, og dermed er det ikke afklaret, hvorvidt bestemmelsen ligeledes omfatter andre former for finansielle midler. Dette kunne eksempelvis være værdipapirer, frimærker eller andet. Det ses dog i tidligere retspraksis, at et andet finansielt middel i form af checks har været anset for omfattet. Dette ses i U.1974.243.Ø.⁹¹ Her ses det, at den tiltalte tilegnede sig checks og kontanter, der herefter blev brugt af den tiltalte. De pågældende checks blev i denne sammenhæng behandlet på samme vis som de kontanter som den tiltalte, også havde tilegnet sig. I og med at checks, i form af at være et andet finansielt middel end penge, blev behandlet på samme vis som de kontanter gerningspersonen havde tilegnet sig, åbnes der her op for at andre finansielle midler også vil kunne være omfattet.

Den strafbare handling skal omhandle betroede penge for at STRFL. § 278, stk. 1, nr. 3, finder anvendelse. I forarbejderne findes der ikke en nærmere beskrivelse af, hvad der forstås ved at pengene skal være betroede. Dog er der tilfælde hvor der ikke kan opstå tvivl. Dette kan eksempelvis være, hvis der deponeres penge i en lukket konvolut, eller hvis pengene ved underliggende aftale, enten stiltiende eller udtrykkelig, skal holdes adskilt fra modtagerens egne midler. Afgørelsen om hvorvidt der er tale om en betroelse, skal træffes ud fra konkret

⁹⁰ LBKG 2022-09-28, nr. 1360, Straffeloven

⁹¹ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 678

fortolkning, ved at tage hensyn til de underliggende individuelle omstændigheder, herunder forskellige aftaler og sædvanetyper.⁹²

3.2.2 - Uretmæssigt forbrug

I forbindelse med at der skal foreligge et uretmæssigt forbrug, er det her også vigtigt at tage højde for hvilken stilling gerningspersonen har. Der kan i sådanne tilfælde være tale om et misbrug af sin stilling som blandt andet advokat, revisor, værge eller kasserer i en forening. Hertil ligger der i bedømmelsen af, hvorvidt en kassemedarbejder har begået pengeunderslæb, en vurdering af om vedkommende har taget pengene fra kassen, herunder om medarbejderen er eneansvarlig for, at den stemmer. Hvis kassemedarbejderen er eneansvarlig for, at vedkommendes personlige kasse stemmer, er det nærtliggende at straffe for underslæb, jf. U.1982.1187/1.V⁹³, hvorimod hvis medarbejderen har taget pengene fra en kasse som medarbejderen ikke personligt hæfter for stemmer, altså en slags fælleskasse, vil der være tale om tyveri, jf. TfK.2010.851/2.Ø.^{94 95}

3.2.3 - Forsæt

Berigelsesforsættet vil være til stede på tidspunktet, hvor gerningspersonen indser at denne udsætter den berettigede for en tabsrisiko.⁹⁶

3.2.4 - Fuldbyrkelse

Pengeunderslæb vil være fuldbyrdet, når pengene er brugt under sådanne omstændigheder, der indikerer at de ikke vil være til stede når de retmæssigt kan opkræves.⁹⁷ Det kan også allerede være i den situation, hvor gerningspersonen blot har besluttet sig for at beholde pengene.⁹⁸ Det beror, som tidligere nævnt, på en konkret vurdering hvornår fuldbyrdelsen vil finde sted, afhængigt af den aktuelle situations omstændigheder.

3.3 - Straffelovens § 280

Herunder vil ordlyden i STRFL. § 280 blive behandlet. Dette sker med baggrund i bestemmelsens afgrænsningsmæssige nærhed med databedrageribestemmelsen i STRFL. § 279 a. STRFL. § 280 kriminaliserer det forhold, hvor en gerningsperson, der har adgang til at handle med retsvirkning for en anden, handler til skade for denne og til fordel for sig selv eller en tredjemand.⁹⁹

⁹² Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 679

⁹³ I dommen U.1982.1187/1.V ses en afløser i et supermarked at have indtastet, at der var blevet udbetalt kontanter for pant til trods for, at dette ikke havde fundet sted

⁹⁴ I dommen TfK.2010.851.Ø ses det, at tiltalte sidder ved en kvikkasse i Bilka. Ud fra konteksten hvor det skrives ”når han sad ved kvikkassen”, vurderes at han ikke selv stod til ansvar for at kassen stemte ved arbejdets afslutning

⁹⁵ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 680

⁹⁶ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 681

⁹⁷ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 682

⁹⁸ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 142

⁹⁹ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 171

Den følgende ordlyd vil herefter behandles for at kunne skabe en forståelse for bestemmelsens gerningsindhold;

”For mandatsvig straffes, for så vidt forholdet ikke falder ind under §§ 276-279 a, den, som for derigennem at skaffe sig eller andre uberettiget vinding påfører en anden formuetab
1) ved misbrug af en for ham skabt adgang til at handle med retsvirkning for denne eller
2) ved i et formueanliggende, som det påhviler ham at varetage for den anden, at handle mod dennes tarv”¹⁰⁰

STRFL. § 280 er i sin ordlyd beskrevet som værende en subsidiær bestemmelse for STRFL. §§ 276 - 279 a. Strafferammen for mandatsvig er dog ikke lavere end disse benævnte bestemmelser.

Det bør fremhæves, at der i litteraturen på området hersker det synspunkt, at der til trods for STRFL. § 280's subsidiære stilling i forhold til STRFL. §§ 276 - 279 a, ikke må straffes i sammenstød for samme beløb. Derudover skal en ellers principal bestemmelse, ikke anvendes hvis det derved kræver en udvidende, eller i øvrigt tvivlsom, fortolkning.¹⁰¹

Der kan ud fra ovenstående betragtning, vurderes at hensigten med at gøre STRFL. § 280 subsidiær i forhold til STRFL. §§ 276 - 279 a, ikke har været at skabe en lex specialis-betragtning i forhold til principalbestemmelserne. Det har blot være formålet at specificere, at der ved brugen af STRFL. § 280 skal betragtes, hvorvidt gerningsindholdet vil være mere passende under de principale bestemmelser, førend man benytter STRFL. § 280.

STRFL. § 280 kriminaliserer mandatsvig i to henseender. I STRFL. § 280, stk. 1, nr. 1 kriminaliseres det forhold, hvor gerningspersonen misbruger en, for gerningspersonen, skabt adgang til at handle med retsvirkning for en anden. I STRFL. § 280, stk. 1 nr. 2 kriminaliseres derimod det forhold, hvor gerningspersonen, ved et formueanliggende, som gerningspersonen har pligt til at varetage, handler imod den forurettedes tarv.¹⁰²

Bestemmelsens nr. 1 og nr. 2 overlapper til en vis grad hinanden - dog vil der i tvivlstilfælde næppe være forskel på hvorvidt nr. 1 eller nr. 2 citeres.¹⁰³

Grundet opdelingen i to kriminaliseringsformer, findes det naturligt først at analysere STRFL. § 280, stk. 1, nr. 1 og derefter nr. 2.

3.3.1 - Straffelovens § 280, stk. 1, nr. 1

Som nævnt ovenfor, kriminaliseres det forhold, hvor gerningspersonen misbruger en, for gerningspersonen, skabt adgang til at handle med retsvirkning for en anden. Denne retsvirkning

¹⁰⁰ LBKG. 2022-09-28, nr. 1360, Straffeloven

¹⁰¹ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 171

¹⁰² Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 172

¹⁰³ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 172

behøves ikke være skabt på baggrund af et retsgrundlag. Derfor kan der her være tale om at denne retsvirkning kan være baseret på lov, forvaltningsakt, aftale eller sågar i en faktisk bestående repræsentationsbeføjelse.

I forarbejderne benævnes konkrete tilfælde, der vil falde under anvendelsesområdet for STRFL. § 280, stk. 1, nr. 1. Her nævnes blandt andet benyttelsen af en blankofuldmagt der er modtaget ved en fejl, salg af et allerede solgt, pantsat eller betalt gældsbrief uden den nødvendige påtegning, og tilsvarende misbrug af den legitimation der ligger i en tinglyst adkomst til en fast ejendom. STRFL. § 280, stk. 1, nr. 1 bør ikke anvendes i situationer, hvor en ansat overskrider sin stillingfuldmagt. Retspraksis er dog ikke entydig angående, i hvilke situationer, valget skal falde på citering ad nr. 1, eller nr. 2.¹⁰⁴

STRFL. § 280, stk. 1, nr. 1, har et særligt anvendelsesområde ved misbrug af eget dankort til at foretage betalinger, når der ikke er dækning på kontoen. Beløbet kan være dækket af den ordning, hvor Nets efter betalingskortaftalen, vil dække beløbet overfor den virksomhed som modtager en betaling, der ikke kan dækkes af forbrugerens indestående. Dette vil have den betydning at betalingsmodtageren ikke vil lide et tab. Der vil i en sådan situation være tale om, at gerningspersonen har handlet med virkning for sin bank, og af denne grund anses dette for mandatsvig overfor banken.¹⁰⁵

3.3.2 - Straffelovens § 280, stk. 1, nr. 2

Som anført ovenfor kriminaliserer STRFL. § 280, stk. 1, nr. 2 det forhold, hvor gerningspersonen, ved et formueanliggende, som gerningspersonen har pligt til at varetage, handler imod den forurettedes tarv.

STRFL. § 280, stk. 1, nr. 2 vil i langt de fleste tilfælde falde ind under et misbrug af stillingen som direktør for et selskab, eller misbrug af stillingen som advokat, fuldmægtig, bestyrer eller værge for en anden. Hvis der er tale om et tilfælde, hvor svigen udøves direkte overfor den person, hvis interesser gerningspersonen skal varetage, er det ikke mandatsvig, men nærmere bedrageri efter STRFL. § 279. Situationen vil være tilsvarende, hvis svigen udføres direkte overfor en juridisk persons styrende organer.¹⁰⁶

Hvis handlingen objektivt set ligger indenfor de aktiviteter, der hører til en stilling, kan dette forhold anses som værende mandatsvig. Eksempelvis kan der være tale om en situation, hvor en bankdirektør bevilger uforsvarlige lån til særdeles risikable foretagender, eller hvor en direktør, grundet personlige forhold, leverer firmaets varer på kredit til en ven.¹⁰⁷

¹⁰⁴ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 697

¹⁰⁵ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 698

¹⁰⁶ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 698, f

¹⁰⁷ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 173

3.3.3 - Forsæt

Der kræves forsæt på tidspunktet for dispositionen. Ligeledes kræves der også berigelsesforsæt. Hvis berigelsesforsættet ikke er til stede, kan der foreligge den mulighed at straffe efter STRFL. § 299.¹⁰⁸ Det bemærkes her, at STRFL. § 299 ikke behandles yderligere i denne afhandling.

3.3.4 - Fuldbyrkelse

Forbrydelsen vil være fuldbrydet, når et faktisk formuetaf tab er indtrådt, eller når den strafbare disposition har fremkaldt en væsentlig risiko for formuetaf tabs indtræden.

3.4 - Straffelovens § 276

Herunder vil der foretages en ordlydsfortolkning af STRFL. § 276. Denne ordlydsfortolkning foretages til trods for at denne bestemmelse i sin ordlyd ikke umiddelbart relaterer sig til STRFL. § 279 a. Dog er det vigtigt at behandle denne, idet der er en større mængde praksis hvori stjålne dankort benyttes til kontanthævninger i en hæveautomat og der her kan stilles spørgsmål ved hvorvidt der er tale om databedrageri ved indtastningen af kode og beløb eller om der er tale om tyveri idet kontanterne udtages.

Tyveribestemmelsen i STRFL. § 276 har følgende ordlyd;

”For tyveri straffes den, som uden besidderens samtykke borttager en fremmed rørlig ting for at skaffe sig eller andre uberettiget vinding ved dens tilegnelse. Med rørlig ting sidestilles her og i det følgende en energimængde, der er fremstillet, opbevaret eller taget i brug til frembringelse af lys, varme, kraft eller bevægelse eller i andet økonomisk øjemed.”¹⁰⁹

I anden del af denne bestemmelse beskrives det hvorledes energimængder også vil kunne være genstand for tyveri. Denne anden del af bestemmelsen er dog ikke videre behandlet nedenfor, da denne ikke vil være relevant for denne afhandling.

3.4.1 - Fremmed rørlig ting

Det første krav som STRFL. § 276 stiller, er at der skal være tale om en fremmed rørlig ting. Ved fremmed forstås, at genstanden helt eller delvist skal tilhøre en anden end gerningspersonen.

Selvom tyveri sker ved borttagelse, har det ingen selvstændig betydning at genstanden skal være rørlig. Hertil kan der henvises til U.1937.376.V, hvor der blev stjålet ral fra en strandbred. Altså vil en genstand der tilsyneladende ikke kan betegnes som løsøre før dens borttagelse, alligevel falde under udtrykket “en rørlig ting”.

¹⁰⁸ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 700

¹⁰⁹ LBKG. 2022-09-28, nr. 1360, Straffeloven

Derudover skal der være tale om en ting, hvilket vil sige at der skal være tale om et fysisk objekt.¹¹⁰

3.4.2 - Økonomisk værdi

I tyveribestemmelsens ordlyd beskrives det, at gerningspersonen skal have taget tingen i sin varetægt ”for at skaffe sig eller andre en økonomisk vinding”¹¹¹. Således lægges der vægt på, at den borttagne genstand har en økonomisk værdi, ud fra en almindelig vurdering.

Det kan ligeledes være ulovligt at tilegne sig ting, som på det legale marked ikke har en økonomisk værdi, hvis denne genstand har en økonomisk værdi på det illegale marked. Dette kan være tilfældet når der tales om tyveri af for eksempel dankort, kreditkort, nummerplader, kørekort og pas.

3.4.3 - Varetægt

Genstanden skal ved borttagelsen være i en andens besiddelse, altså fremmed varetægt, jf. ”uden besidderens samtykke” i bestemmelsen. I langt de fleste tilfælde vil tyveriobjekterne befinde sig på en persons, et selskabs, eller en offentlig myndigheds beskyttede område. Disse kan blandt andet være i huse, haver, butikker og kontorer, hvilket betyder at hvis genstanden befinder sig på en af disse førnævnte områder, anses denne som værende i normal varetægt.¹¹²

Der findes hertil tilfælde, hvor en varetægtssfære følger ejerens ting. Dette gælder for eksempel en håndværkers værktøj eller en studerendes cykel. Denne type varetægt betegnes som værende en personlig varetægt.

Uden for denne sfære ses der at være tilfælde, hvor genstande er uden for de ovenfor nævnte ejendomsområder. Disse kan eksempelvis være en båndsav i en skov eller et rullekabel i en grøft. I sådanne tilfælde vil dette betegnes som værende i midlertidig varetægt.¹¹³

3.4.4 - Forsæt

Det kræves, at der er forsæt til alle led i gerningsindholdet på borttagelsestidspunktet. I og med at tyveribestemmelsen falder under berigelsesforbrydelserne, foreligger der også krav om berigelsesforsæt. Det er grundet ovenstående essentielt at påpege, at der kan forekomme en situation hvor en ”gerningsperson” fejlagtigt tror, at en genstand tilhører vedkommende og derved tager genstanden. I en sådan situation kan vedkommende ikke ifalde strafansvar.¹¹⁴

¹¹⁰ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 656

¹¹¹ LBKG. 2022-09-28, nr. 1360, Straffeloven

¹¹² Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 123

¹¹³ Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014), side 124

¹¹⁴ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 667

3.4.5 - Fuldbyrkelse

Fuldbyrðelsesmomentet for tyveribestemmelsen finder sted, når den rørlige ting borttages fra det sted, hvor den befinder sig, og gerningspersonen i situationen har det nødvendige berigelsesforsæt.

Tyveri anses for fuldbyrðet på et meget tidligt tidspunkt. Det er herved tilstrækkeligt at tage en genstand i lommen. I denne sammenhæng er det vigtigt at påpege, at der er mulighed for at fortryde sin handling og tilbagetræde fra forsøg, jf. STRFL. § 22. Dette kan enten finde sted ved eksempelvis at henvende sig ved kassen for at betale for varen eller lægge denne tilbage på plads.

3.5 - Straffelovens § 301

Følgelig vil STRFL. § 301 ordlyd analyseres, dette er relevant da gerningsindholdet i bestemmelsen i mange tilfælde vil medføre at man enten kan tiltales for forsøg eller fuldbyrðelse af STRFL. § 279 a.

Herfor vil STRFL. § 301 følgende ordlyd behandles;

“Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der med forsæt til uberettiget anvendelse fremstiller, skaffer sig, besidder eller videregiver

- 1) Oplysninger, som identificerer et betalingsmiddel, der er tildelt andre, eller*
- 2) Genererede betalingskortnumre.*

Stk. 2. Sker den i stk. 1 nævnte videregivelse m.v. i en videre kreds eller under i øvrigt særligt skærpende omstændigheder, er straffen fængsel indtil 6 år.

Stk. 3. Bestemmelsen i stk. 1 finder ikke anvendelse på ægte betalingskort.”¹¹⁵

STRFL. § 301 blev indført i 2004. Dette skete på baggrund af, at Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet afgav delbetænkning VIII om IT-kriminalitet i 2002.

Det kriminaliserede indhold i bestemmelsen omfatter fremstilling, anskaffelse, besiddelse eller videregivelse af informationer der identificerer et betalingsmiddel, eller genererede betalingskortnumre. Når forholdet finder sted under skærpende omstændigheder, findes der en skærpet strafferamme i stk. 2.

3.5.1 - “Fremstiller, anskaffer sig, besidder, eller videregiver”

For at kunne ifalde strafansvar efter STRFL. § 301, skal gerningspersonen have fremstillet, anskaffet sig, besiddet eller have videregivet oplysninger, der kan identificere et betalingsmiddel.

Fortolkningen af disse begreber må antages at følge den gængse fortolkning af ordenes betydning, således ses det brugt i retspraksis, jf. TfK.2018.751.V. Det ses i denne dom, at de

¹¹⁵ LBKG. 2022-09-28, nr. 1360, Straffeloven

tiltalte havde installeret teknisk udstyr på flere bankers betalingsautomater, der kunne kopiere og gemme de oplysninger på de betalingsmidler der blev brugt i hæveautomaten. Herved anskaffes og besiddes oplysningerne. Det nævnes ligeledes at disse anskaffede informationer skulle bruges af gerningspersonerne selv, eller en uidentificeret medgerningsperson, hvori videregivelsen ligger.

3.5.2 - Straffelovens § 301, stk. 1, nr. 1.

Her kriminaliseres det forhold, hvor gerningspersonen fremstiller, anskaffer sig, besidder, eller videregiver oplysninger der kan identificere et betalingsmiddel, der er tildelt andre. Disse oplysninger kan eksempelvis være de informationer, der er lagret i en magnetstribe. Oplysninger såsom kortnummer og CVV- eller CVC-koden, kan bruges til online køb.¹¹⁶

3.5.3 - Straffelovens §301, stk. 1, nr. 2.

Herunder kriminaliseres forholdet hvor gerningspersonen fremstiller, anskaffer sig, besidder, eller videregiver genererede betalingskortnumre.

Dette kan være i tilfælde, hvor gerningspersonen har generet numrene på betalingskort, hvor disse er fundet ved hjælp af en matematisk model, således at de fremtræder som gyldige. Det kan også betyde, at de kan være tilfældige numre, blot placeret på kortet for at skabe troværdighed, for herefter at have inkorporeret de nødvendige betalingsinformationer i magnetstriben.¹¹⁷

3.5.4 - Forsæt

For at kunne blive straffet efter STRFL. § 301, kræver det at gerningspersonen har forsæt, jf. STRFL. § 19 modsætningsvist. I bestemmelsen er det tydeliggjort, at de nævnte handlinger sker med forsæt til uberettiget anvendelse dette er gjort, da der blandt andet ved brug af betalingskortoplysninger, legalt kan købes ting over internettet, også hvis der betales med en anden persons kortoplysninger. Dette kunne være tilfælde, hvor der er tale om samtykke fra ejeren af dankortet.¹¹⁸

3.5.5 - Fuldbyrddelse

STRFL. § 301 er ikke en berigelsesforbrydelse ligesom de ovenstående bestemmelser. Af den grund kræves der her ikke, at gerningspersonen opnår en uberettiget vinding, eller skaber en væsentlig risiko for tab hos den forurettede.

Fuldbyrddelsen i STRFL. § 301 finder sted, når ét af de i straffebestemmelsens nævnte kriterier, finder sted. Altså vil bestemmelsen fuldbyrddes, når gerningspersonen fremstiller, skaffer sig, besidder eller videregiver oplysninger, jf. ovenstående.

¹¹⁶ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 795

¹¹⁷ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 795

¹¹⁸ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 795

Det er afslutningsvist vigtigt at påpege, at anvendelsen af de anskaffede oplysninger, vil straffes efter STRFL. § 279 a.

3.6 - Delkonklusion

I ovenstående gennemgang af de tilstødende paragraffer ses det, at disse grænser op til STRFL. § 279 a. Denne påstand vil gennemgås nedenfor, for at give et klart overblik over, hvordan dette hænger sammen.

STRFL. § 279 grænser, som nævnt ovenfor, naturligt op til STRFL. § 279 a, idet STRFL. § 279 a er bygget op omkring STRFL. § 279. Forskellen mellem disse to bestemmelser er tydeligst i det kriterie, at der i STRFL. § 279 skal foreligge en reel vildfarelse af et andet menneske. i modsætning hertil stilles der i STRFL. § 279 a ikke et krav om, at der skal være en fysisk person, der er offer for en vildfarelse. Hertil kommer, at databedrageribestemmelsen i STRFL. § 279 a, fuldbyrdes langt tidligere end bedrageribestemmelsen i STRFL. § 279. Dette ses både i aspektet hvor der i STRFL. § 279 a indgår den digitale faktor hvis ændring finder sted omgående, hvorimod der ved en vildfarelse af en fysisk person kan gå længere tid, før dette bedrageri rent fysisk finder sted.

Den nærmere afgrænsning for hvornår der begås henholdsvis bedrageri eller databedrageri, behandles i afsnit 4.1.

STRFL. § 278, stk. 1, nr. 3, grænser ligeledes op til STRFL. § 279 a. Når vi taler om pengeunderslæb, vil der i mange tilfælde, især i den moderne digitaliserede verden, hvor STRFL. § 278, stk. 1, nr. 3 vil kunne benyttes på samme vilkår som STRFL. § 279 a. Her bliver det dog essentielt at henvise til det ovenfor beskrevne faktum, at STRFL. § 279 a indeholder aspektet med data, hvilket STRFL. § 278, stk. 1, nr. 1 ikke gør. Af denne grund bør dette aspekt være en guideline for hvornår der begås henholdsvis pengeunderslæb eller databedrageri. Dog er det set i retspraksis, at afgrænsningen mellem disse ikke er fuldstændig klar og enstydig, hvorfor en nærmere analyse af dette, ved hjælp af retspraksis, vil behandles i afsnit 4.2.

STRFL. § 280 kan ligesom ovenstående bestemmelse finde anvendelse på samme forhold som STRFL. § 279 a. Afgrænsningen er herfor vigtig, da der i disse tilfælde vil være tale om, at STRFL. § 279 a vil skulle overvejes før STRFL. § 280, jf. ovenstående gennemgang i afsnit 3.3. Igen kan der lægges vægt på det data aspekt der foreligger i STRFL. § 279 a, som netop skaber den overordnede adskillelse fra STRFL. § 280. Med henblik på dataelementet i STRFL. § 279 a, er det her essentielt at have for øje, at der før indførslen af STRFL. § 279 a, er blevet benyttet en udvidet fortolkning af STRFL. § 280.

Grundet ovenstående problemstillinger, behandles afgrænsningen mellem STRFL. § 280 og STRFL. § 279 a nærmere i afsnit 4.2.

STRFL. § 276 grænser op til STRFL. § 279 a i den forstand, at der godt kan være tale om, at der opnås en uberettiget vinding, ved tyveri såvel som ved databedrageri. Den distinktive

forskel her er dog, at der ved databedrageri ikke findes et krav om at det borttagende, der skaffer den uberettigede vinding, skal være en rørlig ting. Den uberettigede vinding kan, i forbindelse med databedrageri, fremskaffes som en fysisk ting. Dette kan eksempelvis være tilfældet ved misbrug af dankortoplysninger, der medfører en forsendelse af en fysisk vare.

Grænsen for hvornår der er tale om tyveri til forskel for databedrageri, behandles videre i afsnit 4.3.

Afslutningsvist grænser STRFL. § 301 op til STRFL. § 279 a ved at STRFL. § 301 håndterer de forhold, der ligger forinden STRFL. § 279 a træder i kraft. Dette vil altså sige, at gerningsindholdet i STRFL. § 301, ligger forinden forsøg på databedrageri. En nærmere afgrænsning mellem disse vil finde sted i afsnit 4.5.

Kapitel 4 – Straffelovens § 279 a i praksis

I denne afhandling, er det væsentligt at kigge nærmere på retspraksis, for at finde frem til en afgrænsning af, hvor vidt benyttelsen af databedrageribestemmelsen i STRFL. § 279 a går. I den forbindelse vil det ligeledes blive undersøgt, hvorledes bestemmelsen anvendes i samspil med de ovenfor gennemgåede tilstødende bestemmelser, samt hvordan Anklagemyndigheden benytter STRFL. § 279 a.

I det følgende kapitel vil der blive set på retssager der involverer en afgrænsningsmæssig problemstilling mellem STRFL. § 279 a og de tilstødende bestemmelser, som der er blevet redegjort for i forrige kapitel. Dette er gjort, for at belyse den respektive retspraksis samt tiltalepraksis der foreligger, i de angivne afgrænsningsspørgsmål.

4.1 - Straffelovens § 279 kontra § 279 a

I dette afsnit, vil emnet internethandel blive behandlet, der primært omhandler gerningspersonens køb af goder over internettet. Denne type af kriminelle handlinger analyseres med henblik på at belyse retspraksis' afgrænsning mellem STRFL. § 279 og STRFL. § 279 a.

Det er særligt relevant at klarlægge retspraksis på dette område, da mere og mere handel føres digitalt og dermed bliver berigelseskriminaliteten i den forbindelse, tilsvarende mere digitalt målrettet. Derudover er internethandel ikke isoleret til kun at omfatte handel med goder. Der er også tale om ydelser, som eksempelvis tegning af lån eller investering i diverse investeringsmidler, som er rykket online. Dette gør, at forbrugeren nemmere og hurtigere kan gøre brug af virksomhedernes ydelser, uden at skulle være i fysisk kontakt med forhandleren.¹¹⁹

Begrænsningen af den fysiske kontakt mellem forbruger og forhandler lægger op til en problemstilling, hvor det afgørende spørgsmål er, hvilken bestemmelse der skal dømmes efter, når en gerningsperson handler på en webshop velvidende, at personen enten ikke kan eller vil betale for varen der bestilles. Dertil medtages også situationer, hvor gerningspersonen uberettiget bruger betalingsoplysninger der ikke er personens egne. Omdrejningspunktet for denne type problemstillinger, vil bestå af sondringen mellem, og afgrænsningen af, bedrageribestemmelsen i STRFL. § 279 og databedrageribestemmelsen i STRFL. § 279 a.¹²⁰

På baggrund af ovennævnte problemstilling, vil der udføres en belysning af litteraturens behandling af forholdet samt en afklaring af hvilken bestemmelse domstolene har benyttet ved domfældelse.

4.1.1 - Vildfarelse

Databedrageribestemmelsens gerningsindhold er på mange måder bygget op om bedrageribestemmelsens lovtekniske struktur. Der hvor databedrageribestemmelsens indhold

¹¹⁹ Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 302

¹²⁰ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 695

dog afviger fra bedrageribestemmelsen, er ved vildfarelseskravet som er udeladt i STRFL. § 279 a. Dette skyldes, at der i praksis er flere bedragerilignende problemstillinger der falder udenfor bedrageribestemmelsens anvendelsesområde, da der ikke fremgår en fysisk person der i vildledelse udfører, eller undlader at udfører, en handling.¹²¹

I betænkningen fremgår følgende;

*“For så vidt angår dataforhold vil § 279 om bedrageri omfatte tilfælde, hvor en person uretmæssigt tilføjer, ændrer eller sletter dataoplysninger under omstændigheder, hvor en anden person derefter opfatter de urigtige dataoplysninger og på dette grundlag foretager en handling (...)”*¹²²

Der kan her sammenlignes med situationen, hvor en gerningsperson svigagtigt afgiver urigtige oplysninger eller fremlægger urigtige regninger til en modtager, for at frembringe en disposition. Et eksempel på en sådan problemstilling, kan ses i en utrykt byretsdom fra 1996.¹²³ Her påvirkede bestyrelsesformanden og flere direktører i Nordisk Fjer Holding A/S koncernens regnskab, for at vildlede investorer og banker til at tro, at koncern var mere solid end hvad den faktisk var.¹²⁴ Her ses det, at en svigagtig anbringelse af urigtige oplysninger i koncernens regnskab kunne medføre en disposition hos interessenterne. Dispositionen ville dog være et resultat af en vildledelse, fremkaldt af det ukorrekte koncernregnskab.

Det kan til gengæld ikke antages, at der bør foreligge bedrageri ved retsstridigt køb over internettet, hvor der eksempelvis bliver brugt andre kortoplysninger end gerningspersonens egne. Denne indtastning af kortoplysninger vil nemlig ikke nødvendigvis bringe en anden person i vildfarelse, afhængig af virksomhedens opsætning.¹²⁵

I Straffelovsrådets betænkning fremgår følgende;

*”udenfor § 279 om bedrageri falder alle tilfælde, hvor en forretningsmæssig arbejdsgang er i den grad automatiseret, at der ikke i forløbet optræder en enkeltperson, der handler på grundlag af de urigtige dataoplysninger.”*¹²⁶

På samme måde vil det falde udenfor bedrageribestemmelsens anvendelsesområde, hvis en person udfører en handling baseret på de oplysninger personen får fra en dataterminal, men hvor personens stilling og arbejdsopgave ikke omhandler en prøvelse af de afgivne oplysningers korrekthed.¹²⁷

¹²¹ Lars Bo Langsted og Peter Helbo Langsted, *Hovedlinjer i erhvervsstrafferetten*, (København: DJØF forlag, 2020), side 107

¹²² Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 45

¹²³ Lars Bo Langsted og Peter Helbo Langsted, *Hovedlinjer i erhvervsstrafferetten*, (København: DJØF forlag, 2020), side 99, eksempel 83

¹²⁴ Utrykt byretsdom 1996, stadfæstet ved ligeledes utrykt Østre Landsrets dom 1998

¹²⁵ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 47

¹²⁶ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 47

¹²⁷ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 47

Langsted og Langsted åbner op for spørgsmålet, om hvorvidt den uberettigede brug af andres fysiske kort og betalingskortskoder, eller brugen af eget betalingskort uden den fornødne dækning ved internethandel, skal dømmes efter databedrageribestemmelsen i STRFL. § 279 a. Der argumenteres her for, at hvis transaktionen foretages automatisk, herunder også afsendelsen af varen, må en del af disse situationer dømmes efter databedrageribestemmelsen i STRFL. § 279 a.¹²⁸

4.1.2 - Retspraksis

I nedenstående afsnit vil tre domme der alle omhandler uberettiget brug af betalingskort og betalingskortoplysninger tilhørende andre end gerningspersonen ved internethandel, blive behandlet. Disse domme er udvalgt, da deres indhold viser et billede af, at ikke alle domstole tager stilling til hvorvidt der faktisk foreligger en vildfarelse, eller om virksomhedens drift i det store hele kan karakteriseres som automatiseret.

I Østre Landsrets dom fra 2019 blev en, på gerningstidspunktet, 15-årig marokkansk asylansøger dømt skyldig i blandt andet databedrageri, ved uberettiget at have benyttet et stjålet dankort til betaling i en fysisk butik, ved brug af den kontaktløse funktion på dankortterminalen. Da betalingen foregik i en fysisk butik hvor varen samtidig udleveres, vil forholdet nærmere skulle falde under drageribestemmelsens anvendelsesområde.¹²⁹

På lignende måde fremgår domstolenes manglende stillingtagen i en dom fra Næstved Byret, i 2014, omkring drageri. I denne dom havde gerningspersonen uberettiget benyttet en anden persons kortoplysninger, til at bestille varer på en webshop. Det fremgår ikke af sagens beskrivelse hvorvidt der faktisk forelå en vildfarelse hos en fysisk person eller om transaktionen i det store hele var automatiseret. Hvis det sidstnævnte er tilfældet, vil dommens faktum falde udenfor drageribestemmelsens anvendelsesområde og STRFL. § 279 a vil i stedet finde anvendelse.¹³⁰

Til sidst er der en afgørelse fra 2014, hvor en serbisk statsborger blev kendt skyldig for databedrageri af særlig grov beskaffenhed. Gerningspersonen havde bestilt flere telefoner fra henholdsvis Telenor og Telia, ved uberettiget at have indgivet en andens personlige oplysninger, uden hensigt til at betale for telefonerne. Det er dog vigtigt at fastslå at landsretten og Højesteret kun tager stilling til spørgsmålet om udvisning, hvorfor der lægges vægt på byrettens begrundelse.¹³¹

Disse ovenstående domme skaber et billede af en retspraksis, hvor der er usikkerhed om afgrænsningen mellem drageribestemmelsen i STRFL. § 279 og databedrageribestemmelsen

¹²⁸ Lars Bo Langsted og Peter Helbo Langsted, *Hovedlinjer i erhvervstrafferetten*, (København: DJØF forlag, 2020), side 108

¹²⁹ TfK.2019.1071/2.Ø

¹³⁰ AM.2014.04.23.B

¹³¹ U.2015.3399.H

i STRFL. § 279 a. Dette kan særligt ses i de to sidstnævnte domme, hvor der er lignende faktum og med tidsmæssigt sammenfald, men med vidt forskellige domsfastsættelser.

4.1.3 - Landsrettens afgørelse

Som nævnt i tidligere afsnit, har domstolene været uenige omkring grænsen mellem anvendelsen af bedrageribestemmelsen i STRFL. § 279 og databedrageribestemmelsen i STRFL. § 279 a, og dermed medført et usikkert retspraksisgrundlag. I 2015 blev der endeligt taget stilling til problemstillingen omkring afgrænsningen mellem bestemmelserne, når gerningspersonen retsstridigt påvirker resultatet af en databehandling.

Problemstillingen blev behandlet af Vestre Landsret i 2015. Sagen omhandlede to rumænske statsborgere, der blev dømt for bedrageri og databedrageri af grov beskaffenhed. Faktum i sagen forelå således, at gerningspersonerne, over en kort tid i 2014, sammen med andre rumænske statsborgere, blev ansat i tomme virksomheder for at få opholdstilladelse, sygesikringsbevis, NemID og bankkonto i Danmark. Ansættelserne var standardkontrakter, der alle indeholdt de samme stavfejl og udelukkende brugt for at opnå de nødvendige tilladelser og beviser som de førnævnte. Alle de indrejsende boede på adresser i Midt- og Vestjylland, hvor det var muligt at foretage en hurtig afgang. Adresserne blev efterfølgende brugt til at købe et stort antal varer samt etablere kredit og optagelse af flere lån. De købte varer blev bestilt til adresserne og efterfølgende fjernet, og angiveligt transporteret til udlandet.¹³²

Angående spørgsmålet, om hvorvidt forholdene skulle anses for bedrageri eller databedrageri, anførte retten følgende;

“tilfælde, hvor en person uretmæssigt tilføjer, ændrer eller sletter dataoplysninger, hvor en anden person derefter opfatter de urigtige oplysninger og på dette grundlag handler eller undlader at handle, er som udgangspunkt også omfattet af straffelovens § 279.”¹³³

Dette stemmer overens med Straffelovrådets fortolkning, i betænkningen. Det fastslås, at tilstedeværelsen af vildfarelsen er nødvendig i forhold til at straffe efter STRFL. § 279.

Retten anførte endvidere at;

”straffelovens § 279 a om databedrageri indeholder derimod ikke som § 279 et krav om, at en person som følge af gerningsmandens forhold skal være blevet vildledt til at foretage en disposition. I stedet for denne vildledning træder ved databedrageri et indgreb i grundlaget for den elektroniske databehandling. Retsstridig tilføjelse af oplysninger til en virksomheds it-system i forbindelse med køb, lånoptagelse og etablering af kredit hos virksomheden over internettet må antages som udgangspunkt at være omfattet af straffelovens § 279 a om

¹³² TfK.2015.906.V

¹³³ TfK.2015.906.V

databedrageri. Herved sker der tilføjelse til og påvirkning af elektronisk databehandling og dermed indgreb i grundlaget herfor.”¹³⁴

Vestre Landsret fandt, at der i to af forholdene omkring køb på kredit, var udført personlig henvendelse og betjening, og derfor var disse omfattet af bedrageribestemmelsen i STRFL. § 279. Retten begrundede, at der ved den ovenfor anførte argumentation kunne anses, at forholdene stemte overens med karakteren omfattet af STRFL. § 279. De øvrige køb, lånoptagelserne og kreditetableringen i forholdene, var begået ved brug af en computer og en internetforbindelse til at skabe kontakt til den pågældende virksomheds IT-system, for derefter retsstridigt at afgive oplysninger til samme system. Retten fandt, at systemerne derefter blev behandlet og godkendt via en automatiseret proces, uden en ansat i virksomheden skulle efterprøve oplysningernes rigtighed. På den baggrund fandt retten, at de pågældende handlinger var omfattet af databedrageribestemmelsen i STRFL. § 279 a, og dermed faldt udenfor bedrageribestemmelsen.¹³⁵

Hvad der er afgørende at uddrage fra denne dom, er at domstolens argumentation stemmer overens med Straffelovrådets begrundelse i betænkningen fra 1985, om hvorvidt der foreligger en menneskelig behandling af ordren, og om denne behandling reelt omhandler en afprøvelse af oplysningernes validitet. Det må derfor findes antageligt, at en ansat af underordnet stilling hvis arbejdsopgaver begrænses til den blotte udførsel af instruks fra et datasystem, ikke kan anses at reelt afprøve oplysningernes rigtighed, og dermed ikke kan anses for at være vildledt.¹³⁶

4.1.4 - Ændring af tiltalepraksis

Den ovennævnte dom fik stor betydning for fremtidig retspraksis, med sin afgrænsning mellem bedrageri- og databedrageribestemmelsen. Dommens relevans var særlig tydelig i en ankesag fra Østre Landsret.¹³⁷ Her havde gerningspersonen i 2013 blandt andet stjålet et Visa/Dankort, og udnyttet kortet til at bestille en rejse fra Spies A/S via internettet. Dette medførte, at Spies A/S led et formuetab. Tiltalen lød indledningsvist på bedrageri efter STRFL. § 279 ved;

“at skaffe sig eller andre uberettiget vinding, i forening og under anvendelse af oplysninger fra det i forhold 1 nævnte Visa/Dankort, retsstridigt, via internettet at have formået Spies A/S til at sælge dem en rejse til en værdi af 53.660 kr., idet de fremkaldte den vildfarelse, at de var berettigede til at bruge kortet, hvorved Spies A/S led et formuetab på 7.198 kr.”¹³⁸

Ved den efterfølgende ankesag ved Østre Landsret, ønskede Anklagemyndigheden forholdet henført som overtrædelse af STRFL. § 279 a, altså databedrageribestemmelsen.¹³⁹

¹³⁴ TfK.2015.906.V

¹³⁵ TfK.2015.906.V

¹³⁶ TfK.2015.906.V og Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 695

¹³⁷ TfK.2015.289.Ø

¹³⁸ TfK.2015.289.Ø

¹³⁹ TfK.2015.289.Ø

Østre Landsret anførte i sin begrundelse omkring afgørelsen af Anklagemyndighedens påstand, at;

*“det lægges til grund, at tiltalte gjorde brug af kortet via internettet og retsstridigt søgte at påvirke resultatet af elektronisk databehandling for derigennem at skaffe sig eller andre uberettiget vinding. Forholdet 3, i hvilket tiltalte findes skyldig som i øvrigt fastslået af byretten, henføres herefter som overtrædelse af straffelovens § 279 a om databedrageri.”*¹⁴⁰

Rettens afgørelse illustrerer, at Anklagemyndigheden har været opmærksom på Vestre Landsrets afgørelse i den førnævnte dom¹⁴¹, samt begrundelsen for afgrænsningen mellem bedrageri- og databedrageribestemmelsen og hvorefter Anklagemyndigheden valgte at ændre tiltalens grundlag ved ankesagen.

4.1.5 - Opsummering

Efter ovenstående analyse af henholdsvis den juridiske litteratur og relevant retspraksis, konkluderes det, at det afgørende moment i afgrænsningsspørgsmålet mellem bedrageribestemmelsen i STRFL. § 279 og databedrageribestemmelsen i STRFL. § 279 a's anvendelse, må anses at være spørgsmålet om vildfarelsesbetingelsen.

I de situationer, hvor gerningspersonen foretager sit køb på internettet ved uberettiget brug af en andens kortoplysninger eller urigtige kortoplysninger, og hvor virksomhedens driftsmæssige proces er automatiseret, eller at betalingsoplysningerne ikke efterprøves af den fysiske person der måtte behandle den pågældende ordre, vil forholdet da falde under STRFL. § 279 a om databedrageri. Dette understøttes af betænkningen, der netop fastslår at bedrageritilfælde af denne type vil kunne falde udenfor STRFL. § 279, og dermed udgør formålet for indførslen af databedrageribestemmelsen.¹⁴²

Antagelsen omkring vigtigheden af vildfarelsesmomentets i afgrænsningsspørgsmålet, understøttes til lige af Elholm, Madsen, Rahbæk og Røn.¹⁴³ De argumenterer for, at misbruget af et datasystem blandet med et bedragerimoment og et vildfarelsesmoment kan finde sted, og at STRFL. § 279 a i de tilfælde ikke udelukker anvendelsen af STRFL. § 279.¹⁴⁴ I deres argumentation fremlægger de, at i situationer hvor datasystemet egentlig mere udgør en kommunikationskanal, end hvad det udgør en automatiseret proces, vil forholdet falde under bedrageribestemmelsens anvendelse, da der i så fald vil være en konkret forholdelse til oplysningerne.¹⁴⁵

¹⁴⁰ TfK.2015.289.Ø

¹⁴¹ TfK.2015.906.V

¹⁴² Betænkning nr. 1032, (København, 1985), *Straffelovrådets betænkning om datakriminalitet*, side 47

¹⁴³ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 695

¹⁴⁴ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 695

¹⁴⁵ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 695

Som tidligere nævnt, argumenterer Lasse Lund Madsen, i sin artikel fra 2016, at det skal gøres klart, at der ikke foreligger en fuldstændig sikker afgrænsning mellem de to bestemmelser, men at afgrænsningen indtil videre vil være flydende. Derudover fastslår han, at det i visse situationer vil være en retsmæssig smagssag, om hvorvidt forholdet falder under enten bedrageri- eller databedrageribestemmelsen.¹⁴⁶

Det anses på nuværende tidspunkt at grænsen mellem bedrageribestemmelsen i STRFL. § 279 og databedrageribestemmelsen i STRFL. § 279 a, fremgår forholdsvis klart, baseret på ovenstående behandling af problemstillingen ved bedrageri vedrørende internethandel. Det vurderes, at en ensartet tiltalepraksis er værd at efterstræbe, da det både vil øge borgernes retssikkerhed, selvom strafferammen er ens for begge bestemmelser, jf. STRFL. §§ 285-287, men også grundet den digitale udvikling, som ses ved berigelsesforbrydelserne.

4.2 - Straffelovens § 278, stk. 1, nr. 3 og § 280 kontra § 279 a vedrørende ansættelsesforhold

Den næste problemstilling der behandles, er forhold hvor en ansat udfører uberettigede pengeoverførsler til sig selv eller andre, i led af personens ansættelsesforhold, samt forhold hvor den ansatte disponerer på vegne af den arbejdsgivende virksomhed, eller dennes kunder. Denne type af domme analyseres med det formål at belyse den praktiske afgrænsning mellem STRFL. § 278, stk. 1, nr. 3, STRFL. § 280 og STRFL. § 279 a.

4.2.1 - Indledende bemærkninger

Før dette afsnits behandling påbegyndes, er det relevant at fastslå at afsnittet vil omfatte en større gennemgang af retspraksis end de øvrige afsnit i denne afhandling. Dette er grundet manglen på retspraksis, hvor domstolene tager stilling til afgrænsningen mellem de tre straffebestemmelser, der omfattes af dette afsnits forhold. Af denne grund findes det nødvendigt at gennemgå en større mængde retspraksis, for at kunne danne et tilstrækkeligt billede af afgrænsningsproblematikken.

Som anført i afsnit 2.1 omkring tilblivelsen af databedrageribestemmelsen, her belyst hvordan den uberettigede påvirkning af en databehandling, og hvor gerningspersonen er omfattet af et ansættelsesforhold med den forurettede virksomhed, typisk vil falde ind under STRFL. § 278, stk. 1, nr. 3 om pengeunderslæb og STRFL. § 280 om mandatsvig, før STRFL. § 279 a blev indført. Denne beskrivelse anses også at være gældende i forhold udenfor ansættelsesforholdet, men hvor der stadig foreligger en betroelse af en formue til en enkeltperson.¹⁴⁷

Endvidere er det tidligere blevet belyst, hvordan der ved indførslen af databedrageribestemmelsen, var en intention om at få bestemmelsen til at omfatte de tilfælde, der ville være omfattet af henholdsvis STRFL. § 278, stk. 1, nr. 3 og STRFL. § 280. Grundet forholdets elektroniske karakter, ville disse dog falde udenfor bestemmelse

¹⁴⁶ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 2

¹⁴⁷ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 51

anvendelsesområde, da pengeunderslæb- og mandatsvigbestemmelsen ikke er udformet til at skulle omfatte datakriminalitet.¹⁴⁸

I de følgende afsnit vil retspraksis omhandlende STRFL. § 278, stk. 1, nr. 3, § 279 a og § 280, blive behandlet. Dommene vil omhandle forhold omkring ansattes uberettigede pengeoverførsler fra arbejdsgiveren, forhold hvor der foreligger en uberettiget disposition overfor arbejdsgiveren eller dennes kunder og slutteligt forhold der ikke omfatter ansættelsesforhold, men på samme måde omfatter et betroelsesforhold.

Afhandlingen vil efterfølgende tage stilling til grundlaget for de enkelte dommes afgørelser og hvorvidt der kan udledes en generel afgrænsning mellem databedrageribestemmelsen og STRFL. § 278, stk. 1, nr. 3 og STRFL. § 280's benyttelse i praksis.

4.2.2 - Retspraksis vedrørende straffelovens § 279 a

4.2.2.1 - Uberettigede dispositioner i ansættelsesforhold

Som det blev opsummeret i forrige afsnit omkring hvordan der ved indførslen forelå en intention om at STRFL. § 279 a skulle omfatte forhold der tidligere faldt under STRFL. § 278, stk. 1, nr. 3 og § 280's anvendelsesområder men indeholdt en digital karakter. STRFL. § 279 a er i overensstemmelse hermed blevet anvendt i praksis, i forhold hvor ansatte har overført pengebeløb til sig selv eller andre, eller i lignende situationer.

I dommen TfK.2010.785.V, blev en bogholder tiltalt og dømt for databedrageri af grov beskaffenhed ved, over en 6-årig periode, at have overført i alt 857.000 kroner fra sin arbejdsgivers konti til sin egen, ved brug af elektroniske overførsler. Lignende omstændigheder kan ses i dommen TfK.2004.539.Ø, hvor en kommunal leder, ligeledes over en 6-årig periode, overførte i alt 3.869.825 kroner til et orkestres konto, som den tiltalte havde rådighed over, for senere at hæve de pågældende overførte beløb.

For en sag fra nyere tid, kan der henvises til en dom fra 2017. Her blev den tiltalte dømt for databedrageri, ved uberettiget at have tilegnet sig sin arbejdsgivers betalingskortoplysninger, for derefter at bruge oplysningerne på adskillige indkøb, overførsler til andre personer og virksomheder samt køb af billetter til en forlystelsespark.¹⁴⁹

Udover de forhold der foreligger i de førnævnte domme, foreligger der også en variant, hvor gerningspersonen, grundet vedkommendes stilling, har misbrugt en given adgang, til et IT-system hvorved gerningspersonen indtaster urigtige oplysninger, for at få systemet til at foretage en given handling. Dette kan eksempelvis være tilfælde, hvor gerningspersonen opretter poster i virksomhedens IT-system, til at udføre udbetaling til en borger eller en anden

¹⁴⁸ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 49-50

¹⁴⁹ TfK.2017.9.V

ansat, men hvor gerningspersonen ændrer i modtagerens oplysninger, så overførslen går til en konto som gerningspersonen, eller en af dennes familiemedlemmer, har rådighed over.¹⁵⁰

I Østre Landsrets dom, U.1997.246.Ø, blev den tiltalte dømt for databedrageri ved at, i led af sin stilling som kasserer i en ejerforening, have oprettet fiktive handler med obligationer, via ejerforeningens edb-system. Herved blev der overført store summe fra både ejerforeningens og andelskassens konti, til gerningspersonens egen konto.¹⁵¹

I dommen TfK.2011.184.Ø blev gerningspersonen dømt for databedrageri ved, i led af sin stilling som lønchef, at have oprettet fiktive feriepengeanvisninger på tidligere ansatte i virksomheden gennem virksomhedens edb-system. Herefter anviste gerningspersonen overførslerne til sig selv, og fik dermed overført i alt 3.342.812 kroner fra virksomhedens feriekonto til sin egen konto.¹⁵²

I Højesterets dom, U.2005.666.H, blev den tiltalte dømt for at have begået databedrageri ved, som led af sin stilling som skadebehandler i et forsikringsselskab, at oprette urigtige erstatningsudbetalingsoverførsler via selskabet it-system, for efterfølgende at anføre sit eget tidligere navn og sin partners adresse i erstatningsudbetalingernes modtageroplysninger. Herefter udstedte gerningspersonen checks på op til 5.000 kroner, som vedkommende selv indløste og indsatte beløbene på sin egen konto. Gerningspersonen tilegnede sig uberettiget i alt 1.282.446 kroner.¹⁵³ Lignende forhold fandt sted i dommen TfK.2004.282.Ø.

4.2.2.2 - Uberettigede dispositioner overfor kunder

Ved dispositioner foretaget over for kunder, hvor gerningspersonen overfører penge fra disses konti til sig selv, kan lignende forhold som ovenfor gøres gældende.

I dommen U.1989.708 blev gerningspersonen, der var ansat som sparekasseassistent, dømt for databedrageri, ved at have udført 190 uberettigede transaktioner fra i alt 31 kundekonti til egen konto, betaling af egne regninger samt til hævnninger ved kassen. I alt tilegnede gerningspersonen sig 106.073,64 kroner.¹⁵⁴

En lignende dom fra 2004 viser, at en bankrådgiver i et pengeinstitut blev dømt for databedrageri ved at have overført penge fra i alt ca. 60 kundekonti til sin egen eller andres konti. Det samlede udbytte udgjorde ca. 1,2 mio. kroner.¹⁵⁵

En lidt mere speciel situation ses i en dom fra 2010. Her blev en ansat på en tankstation dømt for databedrageri, ved at have tilegnet sig kortoplysningerne fra to kunder, hvorefter

¹⁵⁰ Eksemplet bygger på Straffelovrådets beskrivelse af en almindelig form for datakriminalitet, i Straffelovrådets betænkning 1032/1985, side 46

¹⁵¹ U.1997.246.Ø

¹⁵² TfK.2011.184.Ø

¹⁵³ U.2005.666.H

¹⁵⁴ U.1989.708

¹⁵⁵ U.2004.2733.H

gerningspersonen svigagtigt misbrugte oplysningerne til at oprette bankkonti i de forurettedes navne. Efterfølgende overførte gerningspersonen henholdsvis 95.847 kroner og 19.677 kroner til de nyoprettede bankkonti, som den tiltalte havde rådighed over.¹⁵⁶

4.2.2.3 - Øvrige betroelsesforhold

Hvad der kan ses at karakterisere de ovenstående domme, er det faktum at disse forhold er udført som led i et ansættelsesforhold. Anvendelsen af STRFL. § 279 a er dog ikke isoleret til kun at omhandle ansættelsesforhold, men finder også anvendelse i tilfælde hvor der foreligger andre betroelsesforhold.

I dommen TfK.2017.1158/2.Ø¹⁵⁷ blev gerningspersonen, der var økonomisk værge for den forurettede, dømt for uberettiget at have overført 6,3 mio. kroner fra den forurettedes konto til sin egen eller sin samlevers konto. Derudover havde gerningspersonen ligeledes overført 2,4 mio. kroner til en tredjepart, for at dække gerningspersonens private indkøb.¹⁵⁸

På trods af, at Straffelovrådets betænkning argumenterer for, at indførelsen af STRFL. § 279 a vil gøre anvendelsen af STRFL. § 278, stk. 1, nr. 3 og STRFL. § 280 mindre hensigtsmæssig i de tilfælde, hvor forholdet omhandler brugen af et datasystem, viser retspraksis noget andet. Denne viser, at STRFL. § 278, stk. 1, nr. 3 og STRFL. § 280 stadig kan finde anvendelse på trods af Straffelovrådets bemærkninger.¹⁵⁹ Disse vil blive analyseret i de efterfølgende afsnit, hvor STRFL. § 278, stk. 1, nr. 3 først vil blive behandlet, og derefter STRFL. § 280. De følgende analyser udføres med henblik på at skabe et overblik over de omhandlende straffebestemmelser afgrænsning, for herigennem at kunne udlede en generel afgrænsning i praksis.

4.2.3 - Retspraksis vedrørende straffelovens § 278, stk. 1, nr. 3

4.2.3.1 - Uberettigede dispositioner i ansættelsesforhold

Først bør dommen TfK.2016.779.Ø fremhæves, hvor en revisor blev dømt for, som statsautoriseret revisor, at have tilegnet sig 780.000 kroner fra sine klienters konti, som vedkommende havde rådighed over, til sin egen konto.¹⁶⁰

På samme måde blev gerningspersonen i dommen TfK.2014.577.V dømt for, som bogholder, at have overført i alt 4.856.975,80 kroner til både sin egen, familiemedlemmers og egne virksomheders konti, samt konti tilhørende tredjeparter for betaling af gerningspersonen og dennes kones regninger.¹⁶¹

¹⁵⁶ TfK.2010.494.Ø

¹⁵⁷ Denne dom er tidligere blevet behandlet i afsnit 2.3

¹⁵⁸ TfK.2017.1158/2.Ø

¹⁵⁹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 49-50

¹⁶⁰ TfK.2016.779.Ø

¹⁶¹ TfK.2014.577.V

Samme forhold ses i dommen TfK.2011.634/2.V, hvor en regnskabschef blev dømt for at have overført penge fra sin arbejdsgivers konto til sin egen, for dels at betale restskat og dels til personlige indkøb.¹⁶²

Et lidt anderledes forhold, ses i dommen TfK.2013.1080.V, hvor gerningspersonen, som led i sin stilling som supermarkedsbutikschef, havde udskrevet online spillekuponer fra butikkens terminal uden at foretage betaling af disse, men bogførte de manglende betalinger på forskellige inaktive konti.¹⁶³

4.2.3.2 - Uberettigede dispositioner overfor borgere

I dommen U.2000.1468.Ø blev gerningspersonen, som var hjemmehjælper, fundet skyldig i, at have misbrugt en fuldmagt til at hæve flere store beløb fra en borgers konto, som gerningspersonen tilegnede sig. Lignende forhold var tilstedeværende i dommen U.1998.182.Ø.

4.2.3.3 - Øvrige betroelsesforhold

I dommen TfK.2004.35.Ø, hvor forholdet ikke omhandlede et ansættelsesforhold, blev gerningspersonen fundet skyldig i uberettiget at have brugt 11.000 kroner der var i hans varetægt. Disse penge tilhørte retligt en anden person, og skulle sendes til Iran gennem gerningspersonens konto.¹⁶⁴

4.2.4 - Retspraksis vedrørende straffelovens § 280

4.2.4.1 - Uberettigede dispositioner i ansættelsesforhold

I en dom fra 2016, blev gerningspersonen dømt for mandatsvig, ved som led i sin stilling som daglig leder af administrationen i en virksomhed at have overført i alt 1.143.129,67 kroner til sin egen bankkonto fra virksomhedens bankkonto, som gerningspersonen havde rådighed over.¹⁶⁵ Lignende forhold er gældende i dommen TfK.2013.415.Ø hvor gerningspersonen, som direktør i to anpartsselskaber, havde hævet og overført mere end 130 mio. kroner til egen konto.¹⁶⁶

De følgende sager viser tilfælde, hvor der ligeledes er dømt for mandatsvig, jf. STRFL. § 280. Dog omhandler disse domme forhold, der differentierer fra de førnævnte domme, da vindingen er opnået på anden måde end ved pengeoverførsler.

I en dom fra 2011, havde gerningspersonen, en vagtmand, ved flere lejligheder uberettiget brugt sin arbejdsgivers benzinkort til at betale for private køb af benzin, til en værdi af i alt 7.298 kroner.¹⁶⁷ Lignende forhold kan ses i en dom fra 2008, hvor gerningspersonen blev dømt

¹⁶² TfK.2011.634/2.V

¹⁶³ TfK.2013.1080.V

¹⁶⁴ TfK.2004.35.Ø

¹⁶⁵ TfK.2016.1218.V

¹⁶⁶ TfK.2013.415.Ø

¹⁶⁷ TfK.2011.396/2.Ø

for uberettiget at have brugt en lastbil samt et benzinkort, der tilhørte vedkommendes arbejdsgiver.¹⁶⁸

En anderledes dom fra 2004 viser, at en tidligere sportschef for DR blev dømt for at have misbrugt et betalingskort, som DR havde givet vedkommende, til at finansiere private kasinobesøg.¹⁶⁹

4.2.4.2 - Ubertigede dispositioner overfor borgere

I dommen TfK.2016.374.V blev gerningspersonen dømt for, i led af sin stilling som pædagog, at have misbrugt sit mandat til at handle på vegne af to borgeres retsvirkning, ved at have ladet private udgifter dække af borgernes konti. Derudover tog gerningspersonen uberettiget penge fra borgerne, ved at lade private udgifter bogføre i borgernes regnskaber. De ubertigede tilegnede midler løb op i et samlet beløb på 220.000 kroner, fordelt på begge borgere.¹⁷⁰

4.2.4.3 - Øvrige betoelsesforhold

I en dom fra 2017, blev gerningspersonen dømt for at have misbrugt en fuldmagt, som vedkommende havde fået af en ældre, svækket kvinde, til at foretage ubertigede hævninger fra den forurettedes konto, og for at have foretaget et uberettiget salg af den forurettedes værdipapirer.¹⁷¹

4.2.5 - Afgrænsningsproblematikken

Efter en sammenligning af gerningsindholdet i de ovenfor gennemgåede domme, kan der ikke findes et tilstrækkeligt grundlag for hvorfor der i nogle domme anvendes databedrageribestemmelsen mens der i andre anvendes enten STRFL. § 278, stk. 1, nr. 3 eller STRFL. § 280.

Ligeledes fremgår der ikke nogen oplysninger om, at der er foretaget et behandlingsskifte i denne type sager, der skulle kunne forklare fremgangsmåden hvor man anvender den ene straffebestemmelse frem for den anden.

Der kan heller ikke lægges til grund, at gerningspersonens stilling skulle være argumenterende for, hvorvidt det er STRFL. § 279 a, § 278, stk. 1, nr. 3 eller § 280 der skal dømmes for, i den givne situation. Igennem de behandlede domme varierer stillingsbetegnelsen for gerningspersonerne sig meget, da det kan observeres at stillingerne spænder fra tankstationsmedarbejdere til revisorer og direktører. Her kan det blot observeres, at der foreligger en tendens til at dømme efter STRFL. § 278, stk. 1, nr. 2, fremfor STRFL. § 280, når forholdet omhandler gerningspersoner med tilknytning til virksomhedens bogholderi. Da dette ikke anses for at være relevant for denne afhandlings undersøgelsesområde, vil observationen ikke blive behandlet yderligere.

¹⁶⁸ U.2008.1063.Ø

¹⁶⁹ U.2004.2870.Ø

¹⁷⁰ TfK.2016.374.V

¹⁷¹ TfK.2017.124.Ø

Som det tidligere er blevet beskrevet i denne afhandling, beskriver Straffelovrådet, at indførslen af databedrageribestemmelsen, vil eliminere sondringen om hvorvidt der er sket en overtrædelse af STRFL. § 278, stk. 1, nr. 3 eller STRFL. § 280. Det er nemlig ikke gerningspersonens stilling der skal afgøre hvordan sagens forhold skal bedømmes, men hvorvidt der har foreligget en påvirkning af et elektronisk datasystem der er det afgørende moment.¹⁷² Ligeledes fjernes problemstillingen om hvorvidt gerningspersonen havde misbrugt dennes stilling eller ej, da den elektroniske databehandling vil medføre, at forholdet kan henføres under samme straffebestemmelse.¹⁷³

Det vurderes derfor at de førnævnte domme, hvor der er sket afgørelse efter STRFL. § 278, stk. 1, nr. 3 og STRFL. § 280, rettelig burde have været henført under databedrageribestemmelsen i STRFL. § 279 a. Dette kan begrundes i, at alle dommene omhandler forhold hvor der er sket en elektronisk databehandling for at opnå en vinding. Det kan både være ved at overføre penge fra en anden parts konto til sin egen konto, den uberettigede brug af benzinkort eller oprettelsen af fiktive udbetalingsposter.

Behandlingen af de førnævnte domme har være begrænset i dens mål om at skabe en forståelse af retspraksis på det angivne område, da størstedelen af dommene er tilståelsessager. Derfor har domstolene ikke fundet det relevant at tage stilling til, hvorvidt den rette subsumption er foretaget, da anklageskriftet har indeholdt gerningsforholdet.

I den tidligere behandlede dom, TfK.2017.1158/2.Ø, lød tiltalen for overtrædelse af STRFL. § 279 a, subsidiært STRFL. § 278, stk. 1, nr. 3 og tertiært STRFL. § 280. Det fremgår dog ikke yderligere af landsrettens begrundelse eller afgørelse, hvorfor den vælger at dømme efter databedrageribestemmelsen fremfor de andre bestemmelser. Det fremgår dog af gerningsindholdsbeskrivelsen, at forholdet omhandler elektronisk pengetransaktion fra den forurettede til gerningspersonen, og det må derfor også anses for at være det mest nærliggende at dømme efter STRFL. § 279 a. Dog kommenterer retten ikke nærmere på afgrænsningen mellem denne bestemmelse og de to tilstødende bestemmelsers anvendelse.¹⁷⁴ En mulig begrundelse må ligge i, at gerningsindholdet har kunnet være indeholdt af anklageskriftet og at dette har været åbenlyst for retten, hvorfor den ikke har fundet det nødvendigt at behandle afgrænsningsspørgsmålet.

4.2.6 - Opsummering

Efter den ovenstående behandling af de tre straffebestemmelser STRFL. § 279 a, § 278, stk. 1, nr. 3 og § 280, må det antages at retspraksis ikke er enstemmig sikker på hvilken bestemmelse der vil være mest nærliggende at dømme efter.

¹⁷² Betænkning nr. 1032, (København 1985), Straffelovrådets betænkning om datakriminalitet, side 49-50 og 57-58

¹⁷³ Betænkning nr. 1032, (København 1985), Straffelovrådets betænkning om datakriminalitet, side 49-50 og 57-58

¹⁷⁴ TfK.2017.1158/2.Ø

Det har derfor efter denne behandling ikke været muligt at kunne foretage en konkret udledning af, hvorvidt en tiltalerejsning efter STRFL. § 279 a fremfor henholdsvis STRFL. § 278, stk. 1, nr. 3 eller STRFL. § 280, er mest korrekt. Derfor må afhandlingens argumentation læne sig op ad hvad den juridiske litteratur kommer frem til, selvom denne dog er sparsom. Her fremgår det, som tidligere nævnt, at dispositioner hvor gerningspersonens handlinger kunne omfattes af STRFL. § 278, stk. 1, nr. 3 og STRFL. § 280, bør subsummeres under databedrageribestemmelsen i STRFL. § 279 a, når forholdet omhandler en påvirkning af en elektronisk databehandling.

4.3 - Straffelovens § 276 kontra § 279 a

Den næste forholdskategori der vil blive behandlet, omhandler en særlig omdiskuteret problemstilling, angående afgrænsningen mellem STRFL. § 276 om tyveri og STRFL. § 279 a om databedrageri. Forholdene omhandler blandt andre den uberettigede benyttelse af et stjålet betalingskort, for derefter at foretage kontante hævnninger. Det kan også være tilegnelsen af en anden fysisk genstand, som eksempelvis tilegnelsen og benyttelsen af et stjålet benzinkort ved en tankautomat.¹⁷⁵ Denne problemstilling vil dog ikke blive behandlet yderligere i denne afhandling. Situationen er blot nævnt, for at konstatere at problemstillingen behandles på samme måde.

Gerningsforholdet omfatter så vidt både den uberettigede brug af ægte fysiske betalingskort, som det omfatter brugen af falske fysiske betalingskort. I retspraksis er det dog anset, at brugen af falske betalingskort er omfattet af databedrageribestemmelsen i STRFL. § 279 a.¹⁷⁶

Indtil for få år siden var den generelle opfattelse, både blandt den juridiske litteratur og blandt domstolene, at forholdet hvor et stjålet kort bliver uberettiget anvendt, skal straffes efter tyveribestemmelsen i STRFL. § 276, i stedet for anvendelsen af databedrageribestemmelsen i STRFL. § 279 a.¹⁷⁷ Det var først ved dommen U.2014.1688.V at landsretten tog stilling til denne afgrænsningsproblemstilling mellem tyveri og databedrageri, i forhold der omhandlede den uberettigede brug af et stjålet betalingskort.¹⁷⁸ Denne dom vil blive yderligere behandlet senere i dette kapitel.

4.3.1 - Straffelovrådets bemærkninger

I betænkningen fra 1985 tog Straffelovrådet ikke endegyldigt stilling til hvornår der foreligger tyveri eller databedrageri, ved den uberettigede anvendelse af et stjålet betalingskort ved en hæveautomat, med henblik på at opnå en kontant udbetaling.¹⁷⁹

Derimod fremførte Straffelovrådet eksempler på hvornår der uden tvivl ville foreligge tyveri. Straffelovrådet fremførte, at en datamaskine, eller en del heraf, samt et datalagringsmiddel eller

¹⁷⁵ Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 305-306

¹⁷⁶ Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 306

¹⁷⁷ Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 306

¹⁷⁸ U.2014.1688.V

¹⁷⁹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 31

et program, alle kunne være objekter for tyveri. Modsætningsvist fastslog Straffelovrådet, at det ville falde udenfor tyveribestemmelsens anvendelsesområde, hvis gerningspersonen blot kopierede et magnetbånd i stedet for at borttage det, da der i det tilfælde ikke vil være sket en borttagelse af en fysisk genstand. Straffelovrådet henviste yderligere til, at forholdet kunne ligne kopieringen af virksomhedsformler eller andet fortroligt materiale.¹⁸⁰

Efterfølgende fremgår det i betænkningen, at der kan opstå en situation, hvor tyveribestemmelsen i STRFL. § 276 muligvis kunne anvendes, ved at en person benytter et falsk betalingskort i en bank med et edb-system implementeret, for at opnå en kontant udbetaling. Straffelovrådet henviser til at dette forhold vil have en vis lighed til den tid, hvor gerningspersoner ville benytte falske mønter i en automat. Denne problemstilling omhandlede dog brugen af falske betalingskort, og Straffelovrådet tog derfor ikke stilling til benyttelsen af stjalne betalingskort.¹⁸¹

4.3.2 - Det forhenværende synspunkt

Det ovenstående forhold har i mange år været anset for at være tyveri, da gerningspersonen har udløst den pågældende maskines mekaniske funktioner, for uberettiget at tilegne sig maskinens beholdning.¹⁸²

Denne opfattelse kan observeres i den tidligere udgave af Kommenteret Straffelov, hvor der argumenteres for at det retteste ville være at anvende tyveribestemmelsen i STRFL. § 276 i tilfælde hvor gerningspersonen uberettiget bruger en andens betalingskort for at tanke benzin på en tankautomat, eller hæve fysiske penge ved en hæveautomat.¹⁸³

Den tidligere udgave af Kommenteret Straffelovs formulering, der sige at det retteste vil være at henhøre forholdet under tyveribestemmelsen, anses af Lasse Lund Madsen at have påvirket tiltalepraksissen, og dermed givet Greve, Jensen og Nielsens synspunkt en særlig autoritativ værdi.¹⁸⁴

4.3.3 - Det nye synspunkt

På lignende måde finder Lasse Lund Madsen at Greve, Jensen og Nielsen udvider tyveribestemmelsens anvendelsesområde i forhold til hvad Straffelovrådet lagde op til i betænkningen 1985/1038.¹⁸⁵ Lasse Lund Madsen fastslår endvidere at der ikke bør herske nogen tvivl om at Straffelovrådet lagde op til, at tyveribestemmelsens anvendelsesområde begrænses i sager omhandlende dataforhold. I forhold til dette siger han;

”Man må formentlig konkludere, at kravet om borttagelse af en fremmed rørlig ting i § 276 giver tyveribestemmelsen et meget mindre anvendelsesområde i dataforhold end

¹⁸⁰ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 31

¹⁸¹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 31-32

¹⁸² Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 306

¹⁸³ Vagn Greve, Poul Dahl Jensen og Gorm Toftegaard Nielsen, *Kommenteret Straffelov – Speciel del*, (København: jurist- og økonomiforbundets forlag, 2012), side 545

¹⁸⁴ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 3-4

¹⁸⁵ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

*bestemmelserne om brugstyveri, bedrageri og mandatsvig. Der ses ikke at være noget behov for ved lovændring at udvide tyveribestemmelsens område med henblik på dataforhold.*¹⁸⁶

Tillige anfører Lasse Lund Madsen at Straffelovrådets formulering i dens analogi med metalstykket, som er nævnt tidligere i dette kapitel, med dens brug af ordet “muligvis” udelukkende åbnede op for at anvendelse af falske betalingskort kan omfattes af tyveribestemmelsen. I praksis har de sager, hvor der er dømt efter tyveribestemmelsen, typisk omhandlet forhold hvor der har været tale om den uberettigede anvendelse af et ægte betalingskort, der er borttaget af gerningspersonen.¹⁸⁷ Som det tidligere er nævnt, vil anvendelse af falske betalingskort for at opnå en vinding, ikke blive behandlet i dette afsnit.

I de efterfølgende afsnit vil der blive gennemgået retspraksis angående denne type forhold, før og efter domstolens stillingtagen til anvendelsesproblematikken i 2014.¹⁸⁸ Det er gjort med det formål at observere hvorvidt senere retspraksis’ afgørelser stemmer overens med den førnævnte dom fra 2014.

4.3.4 - Retspraksis før U.2014.1688.V

Fra indførslen af databedrageribestemmelsen og næsten 30 år frem, herskede den opfattelse, som nævnt i ovenstående afsnit, at forhold hvor et fysisk og ægte betalingskort blev tilegnet af gerningspersonen, for herefter at benytte kortet til at foretage en hævnning af kontanter i hæveautomater, skulle henføres under tyveribestemmelsen i STRFL. § 276. Denne opfattelse stemmer, som tidligere nævnt, overens med Greve, Jensen og Nielsens udvidede fortolkning af tyveribestemmelsens anvendelse.¹⁸⁹

I dommen U.2001.1980/2.H foreligger der et eksempel på Anklagemyndighedens tiltalepraksis, da der forelå tiltale for overtrædelse af tyveribestemmelsen i STRFL. § 276, ved uberettiget at have benyttet sin tidligere samlevers dankort til at hæve i alt 7.000 kroner fra dankortautomater.¹⁹⁰

Lignende forhold gør sig gældende i dommen TfK.2009.48.Ø. Her var der rejst tiltale for overtrædelse af tyveribestemmelsen, ved ni gange at have stjålet betalingskort, efter at den tiltalte først havde afluret koden til de pågældende betalingskort, for derefter at foretage hævnninger med en samlet værdi af 250.000 kroner. Derudover forelå der forsøg på hævnninger, til en værdi på i alt 20.000 kroner.¹⁹¹

4.3.5 - U.2014.1688.V og retspraksis herefter

Ved dommen U.2014.1688.V blev der endeligt taget stilling til subsumtionsspørgsmålet, omkring anvendelsen af databedrageribestemmelsen kontra tyveribestemmelsen.¹⁹²

¹⁸⁶ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 32

¹⁸⁷ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

¹⁸⁸ U.2014.1688.V

¹⁸⁹ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

¹⁹⁰ U.2001.1980/2.H

¹⁹¹ TfK.2009.48.Ø

¹⁹² Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4-5

Sagen omhandlede, som tidligere nævnt i afhandlingen, en gruppe personer der i fællesskab havde oprettet firmaer, og derigennem indgået leveringsaftaler med Nets angående betalingskortterminaler. Gerningspersonerne brugte herefter betalingskortterminalerne til at overføre store summer fra stjalne kort, og kort der ellers var stillet til rådighed. De overførte beløb blev herefter videreoverført til forskellige konti, for derefter at blive hævet eller omsat til guld.¹⁹³

Anklagemyndigheden havde i byretten påstået domfældelse efter STRFL. § 279 a, og havde også fået afsagt dom i overensstemmelse med påstanden. Ved landsretten fremkaldte Anklagemyndigheden af egen drift subsumptionsproblematikken, ved at nedlægge subsidier påstand om tyveri efter STRFL. § 276.¹⁹⁴ Statsadvokatens repræsentant havde endda selv udtalt i sagen, at det ville være mest nærliggende at dømme efter tyveribestemmelsen, og at byrettens afgørelse dermed måtte anses for at være forkert.¹⁹⁵

Landsretten udtalte følgende om subsumtionsspørgsmålet;

“Særligt bemærkes det vedrørende spørgsmålet, om forholdet må anses for databedrageri efter straffelovens § 279 a eller tyveri efter straffelovens § 276, at uberettiget brug af et kort og en terminal til hævning som udgangspunkt er omfattet af straffelovens § 279 a, uanset om transaktionen sker online eller offline. Ved en sådan transaktion sker der påvirkning af resultatet af elektronisk databehandling og dermed indgreb i grundlaget herfor. Derimod indebærer denne form for datakriminalitet typisk ikke, som ved tyveri, borttagelse af en fremmed rørlig ting, jf. Straffelovrådets betænkning om datakriminalitet nr. 1032 1985, side 30 ff. og 80 ff., og forslag til lov om ændring af straffeloven nr. L 221, Folketingstidende 1984/85, Tillæg A, spalte 4373 ff.”¹⁹⁶

Det bliver her klargjort af landsretten, at det centrale ved anvendelsen af databedrageribestemmelsen er hvorvidt der er foretaget en retsstridig påvirkning af resultatet af en databehandling, og herigennem et indgreb i databehandlingens grundlag. Det skal dog gøres klart at landsretten fastslår, at det kun er ved den uberettigede brug af et betalingskort, til hævning ved en betalingskortsautomat, der er omfattet af STRFL. § 279 a.

Lasse Lund Madsen omtaler sagens omstændigheder således, at det er overraskende at Anklagemyndigheden har valgt at fastholde et gammelt synspunkt. Derudover pointerer han, at anklageren selv havde henvist til den daværende version af Kommenteret Straffelov og havde anført at subsumptionsproblematikken allerede var afklaret i retspraksis.¹⁹⁷ Lasse Lund Madsen forklarer, at dette kan være et resultat af, at der blandt nogle jurister ikke findes et tilstrækkeligt klart udtryk for om der menes tiltalepraksis eller retspraksis. Der har netop kun

¹⁹³ U.2014.1688.V

¹⁹⁴ U.2014.1688.V

¹⁹⁵ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5-6

¹⁹⁶ U.2014.1688.V

¹⁹⁷ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

hersket en fast tiltalepraksis til at rejse tiltale efter STRFL. § 276, og derfor har domstolene aldrig taget stilling til problematikken før denne dom.¹⁹⁸

De efterfølgende udgaver af Kommenteret Straffelov, i henholdsvis 2017 og 2022, har siden den omtalte dom¹⁹⁹ skiftet synspunkt, og henviser i den nuværende udgave til, at det forhold, hvor der foreligger et uberettiget brug af et betalingskort til hævnning ved en betalingskortsautomat, må antages at skulle henføres under databedrageribestemmelsen i STRFL. § 279 a.²⁰⁰

I tiden efter kan det observeres, at retspraksis har taget ved lære af U.2014.1688.V, og efterfølgende været opmærksom på at en uberettiget brug af stjålne kort ved hævnninger skulle afgøres efter databedrageribestemmelsen, til trods for den tidligere version af Kommenteret Straffelovs synspunkter.

Der kan her henvises til en dom fra 2015, hvor der var tiltalt for tyveri. Her havde de tiltalte tilegnet sig en andens betalingskort og brugt dette kort til at foretage uberettigede hævnninger. Ved hovedforhandlingerne anmodede Anklagemyndigheden om at anklageskriftet blev berigtiget, så der blev påstået domfældelse efter databedrageribestemmelsen i STRFL. § 279 a, i stedet for tyveri i STRFL. § 276. Byretten afslog anmodningen om berigtigelse med den begrundelse, at det ville udvide tiltalen og dermed krævede samtykke fra de tiltalte. Anklagemyndigheden kærede byrettens beslutning, og landsretten tog kæremålet under påkendelse. Landsretten fastslog, at berigtigelsen blot ville ændre den citerede lovbestemmelse, og at der derfor ikke forelå en ændring af beskrivelsen af det strafbare gerningsindhold. Landsretten henviste til U.2014.1688.V i dens begrundelse for godkendelsen af tiltaleændringen.²⁰¹

Hvilken betydning en sådan korrektion har, vil blive behandlet i kapitel 5 omkring tiltalekorrektion.

4.3.6 - Usikker tiltalepraksis

Der er dog imidlertid stadig, i tiden efter U.2014.1688.V, opstået tilfælde der skaber et billede af at der stadig foreligger tvivl om hvilken lovbestemmelse der skal anvendes i forhold, som dem der er illustreret i kapitlet ovenfor. En af disse er en dom fra 2017.²⁰² Her var der rejst tiltale efter tyveribestemmelsen for at;

”[...] derigennem at skaffe sig eller andre uberettiget vinding, retsstridigt at have påvirket eller forsøgt at påvirke resultatet af en elektronisk databehandling, idet sigtede ved brug af rette kode anvendte det i forhold 12 anførte Mastercard til følgende hævnninger. [...]”²⁰³

¹⁹⁸ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

¹⁹⁹ U.2014.1688.V

²⁰⁰ Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022), side 695

²⁰¹ TfK.2015.443.Ø

²⁰² TfK.2017.934.V

²⁰³ TfK.2017.934.V, forhold 13

Derudover lød tiltalen også på;

”[...] tyveri efter straffelovens § 279 a, samt til dels forsøg herpå”²⁰⁴, ved at ”[...] derigennem at skaffe sig eller andre uberettiget vinding, retsstridigt at have borttaget en fremmed rørlig ting, idet sigtede ved brug af rette kode anvendte det i forhold 27 anførte dankort til følgende hævnninger. [...]”²⁰⁵

Landsretten tog ikke stilling til subsumtionsspørgsmålet da dommen var en tilståelsessag, og derfor dømte landsretten blot i overensstemmelse med anklageskriftet. Det er ikke oplyst hvorfor formuleringen af anklageskriftet viser en sammenblanding af henholdsvis tyveri- og databedrageribestemmelsen, og man kan blot spekulere i årsagen herfor, men det kan skyldes manglende kendskab til den vigtige dom fra 2014.²⁰⁶

Dog viser anklageskriftets formulering, at Anklagemyndigheden har spekuleret over hvorvidt forholdet skulle bedømmes efter tyveri i STRFL. § 276 eller databedrageri i STRFL. § 279 a. Dette ses særligt med formuleringen *”[...] derigennem at skaffe sig eller andre uberettiget vinding, retsstridigt at have påvirket eller forsøgt at påvirke resultatet af en elektronisk databehandling [...]”²⁰⁷* der netop følger databedrageribestemmelsens ordlyd.

4.3.7 - Todeling af gerningsindholdet

Med undtagelse af ovenstående eksempel på et fejlbetonet anklageskrift, kan der observeres en overordnet korrekt tiltalepraksis, hvor der rejses tiltale for databedrageri ved selve benyttelsen af det stjålne hævekort, til foretagelse af hævnninger ved hæveautomater.

Som eksempel herpå kan der henvises til dommen TfK.2015.653.V, hvor den tiltalte erkendte sig skyldig i at have stjålet i alt 23 betalingskort, enten alene eller sammen med andre. Den tiltalte havde forinden tyveriet afluret pinkoden til betalingskortene, og benyttede efter tyveriet disse koder sammen med de stjålne kort, til at hæve penge fra de forurettedes konti. Det samlede udbytte af de retsstridige hævnninger løb op på 380.000 kroner. Anklageren havde i denne sag valgt at opdele gerningsindholdet i henholdsvis tyveriet af betalingskortene og databedrageri ved den uberettigede brug af kortene, ved hævning i hæveautomater.²⁰⁸

Selvom det at henhører selve tyveriet af det fysiske betalingskort under tyveribestemmelsen i STRFL. § 276 og den uberettigede hævning under databedrageribestemmelsen i STRFL. § 279 a kan have en pragmatisk korrekthed, kan det diskuteres hvorvidt en opdeling af forbrydelsen i to dele er hensigtsmæssigt.

²⁰⁴ TfK.2017.934.V, forhold 28

²⁰⁵ TfK.2017.934.V, forhold 28

²⁰⁶ U.2014.1688.V

²⁰⁷ TfK.2017.934.V, forhold 13

²⁰⁸ TfK.2015.653.V

I sin artikel, U.2016B.343, argumenterer Lasse Lund Madsen for, at hvis det ikke er muligt at henføre forholdet under begge bestemmelser, vil det mest korrekte være at henføre forholdet under databedrageribestemmelsen, da det er her vægten af den kriminelle handling foreligger.²⁰⁹ Han forsætter med at sige, at her vil tyveriet blot være en indledende og forberedende handling til det rigtige formål ved forbrydelsen, nemlig brugen af kortet til at foretage hævnninger og få den økonomiske gevinst.²¹⁰ Slutteligt i afsnittet argumenterer han også for, at set ud fra en lex specialis-grundsætning, vil det være mest hensigtsmæssigt at henfører forholdet under databedrageribestemmelsen i STRFL. § 279 a, da denne, er indsat for at opsamle de dragerier som foregår digitalt og ikke en vildfarelse af en fysisk person.²¹¹

I ovenstående dom, TfK.2015.653.V, kan det observeres, at der forelå en uberettiget brug af det stjålne betalingskort ved hævnninger i hæveautomater og at tyngden af det kriminaliserede forhold må tillægges dette. Havde der ikke foreligget en brug af betalingskortet til at foretage en hævning havde det været svært at kunne argumentere for at der egentlig foreligger en uberettiget vinding ved tyveriet.²¹² Dette vil også være tilfældet hvis kortet enten blev solgt videre eller på anden måde brugt i en kriminaliseret handling, hvor den uberettigede vinding opnås ved yderligere handling end blot tyveriet.

Dette understøttes af Lars Bo Langsted i sin artikel fra 2019, hvori han fremhæver at selve tyveriet som udgangspunkt kan straffes efter tyveribestemmelsen i STRFL. § 276 hvis dette gøres i sammenstød med STRFL. § 279, STRFL. § 279 a eller STRFL. § 280, grundet den senere anvendelse.²¹³

4.3.8 - Opsummering

Ud fra den ovenstående redegørelse af retspraksis og den juridiske litteratur, angående brugen af stjålne betalingskort til anvendelse ved hævning i hæveautomater, kan det konkluderes at dette område har opnået en tilstrækkelig strafferetlig beskyttelse gennem den tidligere omtalte præjudicielle dom, der fastslår at denne type forbrydelser skal henføres under STRFL. § 279 a.

Straffelovrådet havde i betænkningen ikke entydigt gjort klart, hvordan sådanne forhold skulle afgøres. Dette er årsagen til, at der først er taget stilling til spørgsmålet om afgrænsningen omkring 30 år efter databedrageribestemmelsens indførsel.

Begrundelsen for hvorfor retspraksis tidligere har dømt efter tyveribestemmelsen i modsætning til databedrageribestemmelsen kan forklares med, at selve gerningsforløbet er begyndt med tyveriet af betalingskortet. Derfor vil det være let for Anklagemyndigheden at komme til den konklusion, at hele gerningsforløbet derfor skal henføres under STRFL. § 276. Denne misforståelse af hvilken bestemmelse der subsumerer hele gerningsforløbet, er på sin vis blevet

²⁰⁹ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²¹⁰ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²¹¹ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²¹² TfK.2015.653.V

²¹³ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 4-5

understøttet af den juridiske litteratur der, som tidligere nævnt, har gjort sit synspunkt om at tyveribestemmelsen var det mest rette at dømme efter tydeligt.

Lasse Lund Madsen skriver i sin artikel at den forhenværende retspraksis medførte en uhensigtsmæssig udvidelse af tyveribestemmelsen, og at denne skævvridning er en meget anderledes fortolkning end hvad Straffelovrådet fremlagde i betænkningen.²¹⁴ Han fortsætter og argumenter for at grunden til U.2014.1688.V, er så skelsættende som den er, er et udtryk for en fastgroet tiltalepraksis der er udviklet fra en fejlfortolkning af databedrageribestemmelsens anvendelsesområde, idet de faktuelle forhold i gerningsforløbet kun på meget begrænset vis afspejler den traditionelle forståelse af tyveribestemmelsen.²¹⁵ Ydermere pointerer han, at det rette er at subsumerer sådanne forhold under databedrageribestemmelsen i STRFL. § 279 a, hvis der ønskes en subsummering.²¹⁶

Siden den præjudicielle dom i 2014²¹⁷, er der sket en stor stigning i antallet af anmeldte sager angående databedrageri i STRFL. § 279 a, indtil 2020 hvor der er sket et fald i anmeldte databedragerier. Dette må anses at være et naturligt og forventeligt resultat af at forhold der tidligere, i statistikken, har været henført under tyveribestemmelsen nu anføres korrekt under databedrageribestemmelsen.²¹⁸

4.4 - Straffelovens § 280 kontra § 279 a

I det forudgående afsnit er der blevet redegjort for hvordan sager der omhandler den uberettigede brug af stjålne kort til hævn i hæveautomater, er blevet afgjort i praksis siden indførslen af databedrageribestemmelsen.

I dette afsnit vil forhold, hvor der foreligger misbrug af eget betalingskort, blive behandlet. Det er tidligere blevet belyst, hvordan den juridiske litteratur havde et skævvredet syn på rækkevidden af tyveribestemmelsens anvendelse. Derudover udtrykte litteraturen, at bestemmelsen kunne subsumere forhold, hvor gerningsindholdet både indeholdt tyveri og databedrageri. Som nævnt udtrykte den tidligere udgave af Kommenteret Straffelov, at det mest korrekte ville være at anvende tyveribestemmelsen i STRFL. § 276. Denne fejlfortolkning i den juridiske litteratur samt retspraksis blev senere rettet, så forhold som disse blev henført under databedrageribestemmelsen i STRFL. § 279 a.

Det må, ud fra den tidligere version af Kommenteret Straffelovs synspunkt, antages at en situation, hvor en person misbruger sit eget betalingskort på en sådan måde, at der foretages et forsætligt uberettiget overtræk på vedkommendes konto, vil falde under samme argumentation som anvendelsen af tyveribestemmelsen. Begrundelsen herfor er, at der sker en tilegnelse af penge fra banken, der som følge af dette lider et tab.

²¹⁴ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

²¹⁵ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 6

²¹⁶ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 4

²¹⁷ U.2014.1688.V

²¹⁸ <https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=38285> – Fald i anmeldte bedragerier – Sidst besøgt d. 11/5 2023

Den modsatte opfattelse foreligger i den nyere juridiske litteratur, hvor det menes at et sådant forhold på korrekt vis skal falde under STRFL. § 280 om mandatsvig. Lars Bo Langsted fremhæver i sin artikel fra 2019, følgende omkring anvendelsen af STRFL. § 280;

”Bestemmelsen vil også være aktuel, hvor den retmæssige kortindehaver trods manglende dækning på kontoen hæver et beløb på op til og med 4.000 kr., fordi Nets via den gældende betalingskortaftale er forpligtet til at godtgøre den virksomhed, der har solgt varen, et beløb til og med 4.000 kr. Gerningsmanden handler på denne måde med retsvirkning for Nets, der også lider tabet.”²¹⁹

Langsted argumenterer videre, at grundet Nets betalingsaftale, hvor Nets står inde for beløb op til 4.000 kroner²²⁰ overfor den kortmodtagende virksomhed, vil der i sådanne situationer skulle dømmes for mandatsvig, for den uberettigede brug af eget kort uden tilstrækkelig dækning. En værdi over dette beløb bør omfattes af databedrageribestemmelsen i STRFL. § 279 a.²²¹

Langsted udtrykker derudover følgende;

”Ved misbrug af eget kort tænkes på en situation, hvor kortholder overtrækker sin konto ved den givne hævnning. Han har f.eks. 2.000 kr. stående på kontoen og anvender sit dankort til at hæve 8.000 kr. som betaling for et fjernsyn [...] [...] Nets via betalingskortaftalen, garanterer over for den modtagende virksomhed, at den vil modtage beløbet op til 4.000 kr., såfremt der er brugt chip og PIN-kode. Kortholder kan på denne måde siges at disponere på Nets' vegne. I modsætning til den gamle checkindløsningsaftale er den kortmodtagende virksomhed garanteret et beløb op til 4.000 kr., også selvom det foretagne træk er som i eksemplet på 8.000 kr. I det tilfælde vil kortholder, såfremt det nødvendige forsæt er til stede, skulle straffes for mandatsvig for de 4.000 kr. og bedrageri, jf. § 279, for de »overskydende« 2.000 kr.”²²²

Det kan her ses, at det centrale i vurderingen om hvornår mandatsvigsbestemmelsen og databedrageribestemmelsen skal anvendes, er Nets betalingsaftale og den garanti Nets indestår, da der så vil foreligge en disposition på Nets vegne.

Det må antages at der kan findes lignende situationer, som det eksempel som Langsted fremhæver, men hvor anvendelsen sker på en sådan måde at der ikke foreligger en fysisk kontakt ved kortbetalingen. I disse tilfælde vil forholdet, i overensstemmelse med argumentationen for anvendelsesafgrænsningen mellem STRFL. § 279 og STRFL. § 279 a, skulle henføres under databedrageribestemmelsen.

²¹⁹ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 2

²²⁰ 2019-sats

²²¹ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 2 og 5

²²² Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 5

Langsted beskriver følgende om anvendelsen af databedrageribestemmelsen i denne type forhold;

*"I øvrigt er grænsen for dækningen, når det er rette kortholder, der bruger kortet, kun på 2.000 kr. ved nethandel. Træk derudover vil også være databedrageri."*²²³

Ved forhold hvor der altså ikke er den fysiske kontakt med en person i den kortmodtagende virksomhed, vil værdien der falder udover de 2.000 kroner blive omfattet af databedrageribestemmelsen.²²⁴

Om gerningspersonen foretager et uberettiget overtræk af sin konto ved flere betalinger, eller i én samlet betaling er underordnet, da de samme garantigrænser gælder for seriebetalinger såvel som én betaling.²²⁵

Langsteds synspunkt på mandatsvigsbestemmelsens anvendelse, kontra drageribestemmelsens anvendelse, følger den tiltalepraksis, som foreligger på det givne forhold, omhandlede misbrug af eget betalingskort. Dette kan eksempelvis observeres i dommen AM2012.02.16B3, hvor den tiltalte havde misbrugt sit eget betalingskort til at hæve kontanter, samt købe forskellige varer og ydelser, uden der var dækning på kortet til disse transaktioner.²²⁶

Lignende tilfælde ses i dommene AM2011.10.31B5 og AM2013.03.19B2, hvor de tiltalte, der blev dømt for mandatsvig, havde foretaget kontante hævninger og køb på deres betalingskort, uagtet at der ikke forelå den tilstrækkelige dækning på betalingskortet, eller overtræksaftale med de tiltaltes banker.²²⁷

Det skal dog nævnes, at disse sager alle er blevet behandlet som tilståelsessager. Domstolene har derfor ikke haft anledning til at skulle tage stilling til tvivlsspørgsmålet, om hvorvidt det er det mest korrekte at dømme efter mandatsvigsbestemmelsen.

4.4.1 - Opsummering

Efter behandling af de forhold der omhandler misbrug af eget betalingskort, som er blevet belyst i ovenstående afsnit, bemærkes det at den juridiske litteratur gennem tiden har udviklet sig fra at sætte tvivlsspørgsmål omkring korrektheden af tiltalepraksissen, til at støtte Anklagemyndighedens praksis.

Særligt den nyere juridiske litteratur fra Langsted understøtter brugen af mandatsvigsbestemmelsen, så længe beløbet ikke overstiger de grænser der foreligger i Nets betalingsaftale. Derudover bliver det også understøttet, at enhver overskridelse af denne

²²³ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 2

²²⁴ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 2

²²⁵ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 5

²²⁶ AM.2012.02.16B3

²²⁷ AM.2011.10.31B5 og AM.2013.03.19B2

grænse, bør omfattes af henholdsvis bedrageri- eller databedrageribestemmelsen, alt efter om kortet er brugt fysisk eller via handel på internettet.

Det vurderes af denne grund, at der ikke på nuværende tidspunkt hersker tvivl om anvendelsesspørgsmålet ved disse forhold. Derfor må Greves synspunkt anses at være styret af, at dankort stadig var en ny opfindelse, samt at den betalingsaftale fra Nets som Langsted bruger til at understøtte sit synspunkt, ikke forelå på det dagældende tidspunkt.²²⁸

Retspraksis afviger fra den juridiske litteraturs synspunkt, ved ikke at anvende databedrageribestemmelsen på det beløb som overstiger dækningen, jf. Nets betalingsaftale. Det observeres herved, at der i de ovenstående analyserede domme, med undtagelse af AM2012.02.16B3, blot er rejst tiltale og dømt efter mandatsvigsbestemmelsen, uden stillingtagen til afgrænsningen mellem denne og databedrageribestemmelsen i STRFL. § 279 a.

4.5 - Straffelovens § 301 kontra § 279 a

Herunder vil begrebet skimming, som er reguleret i STRFL. § 301, blive behandlet. Skimming kan blandt andet foregå på følgende måde;

”Skimming kan foregå ved, at der opsættes udstyr på hæveautomater, som aflæser kortoplysninger og filmer pinkoder, når en person hæver penge i en hæveautomat. Udstyret er ikke umiddelbart synligt. De aflæste oplysninger lagres på hukommelseskort, som kan aflæses, hvorefter der kan fabrikeres falske kort, som der kan hæves penge på eller foretages betaling med.”²²⁹

I det følgende vil der blive redegjort for hvad forsøg på databedrageri dækker over, og herefter vil der foretages en analyse af udvalgt retspraksis, for at kunne klarlægge grænserne mellem benyttelsen af STRFL. § 279 a, jf. § 21 og § 301.

4.5.1 - Forsøg på databedrageri efter straffelovens § 279 a, jf. § 21

Ifølge Knud Waaben kræves det, at gerningspersonen har forsæt til hver enkelt af vedkommendes handlinger der fører til forbrydelsen, før der kan straffes for forsøg. Forsøgsbegrebet i dansk ret er vidtrækkende, og mindstekravet til fuldbyrdet forsøg må ifølge Knud Waaben være, at gerningspersonens beslutninger skal være rettet mod et forløb der kan henføres under en straffebestemmelse, og at disse beslutninger ikke skal være helt ubestemte. Desuden anførtes det af Knud Waaben, at gerningspersonen ikke nødvendigvis skal have planlagt hele gerningsforsøget, så længe gerningspersonen har opfattet at disse handlinger fører til det resultat, at der begås en forbrydelse.²³⁰

²²⁸ <https://www.dankort.dk/dk/om-dankort/> - Fakta om Dankort – Sidst besøgt d. 11/5 2023 og <https://denstoredanske.lex.dk/Nets> - Nets - Sidst besøgt d. 11/5 2023

²²⁹ TfK.2011.388.Ø

²³⁰ Knud Waaben, *Strafferettens almindelige del I – Ansvarslæren*, (København: Karnov Group, 2015), side 227

Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet undersøgte i 2002, hvorvidt der var et behov for at indføre nye bestemmelser i straffeloven. Hertil undersøgte det hvorvidt der i tilfælde, hvor bestemmelsen om forsøg er anvendelig, i dag kan være behov for en mere fremskudt regulering, der ikke er afhængig af, om der kan føres tilstrækkeligt bevis for forsøg.²³¹

Udvalget har efter de ovenfor nævnte overvejelser besluttet at foreslå indsættelsen af en selvstændigt kriminaliserende STRFL. § 301, med følgende ordlyd;

”Med bøde eller fængsel indtil 6 måneder straffe den, der med forsæt til uberettiget anvendelse producerer, skaffer sig, besidder eller videregiver oplysninger, der identificerer et betalingsmiddel, der er tildelt andre, eller genererede betalingskortnumre.

Stk. 2. Sker den i stk. 1 nævnte videregivelse i en videre kreds eller under i øvrigt særligt skærpede omstændigheder, er straffen fængsel indtil 4 år.

Stk. 3. Bestemmelsen i stk. 1 finder ikke anvendelse på ægte betalingskort.”²³²

Udover en ændring af ordet ”producerer” til ”fremstiller” og en skærpelse af strafferammen efter stk. 2 fra 4 til 6 år, forblev lovforslaget uændret ved vedtagelsen.²³³

Fordi der kræves forsæt til uberettiget brug, for at ifalde strafansvar efter STRFL. § 301, fortsætter udvalget med at forklare, at der til forskel fra benyttelsen af STRFL. § 279 a, jf. § 21, her ses bort fra konkretiseringskravet. Derudover har udvalget fundet det mest korrekt særskilt at nævne besiddelse, til trods for at udvalget er klar over, at besiddelse typisk vil indgå i produktion, forskaffelse og videregivelse.²³⁴

Idet der ses bort fra konkretiseringskravet ved benyttelsen af STRFL. § 301, vil det, for at kunne dømme efter STRFL. § 279 a, jf. § 21, kræves at Anklagemyndigheden kan bevise at gerningspersonens konkrete plan var at ændre, tilføje eller slette oplysninger eller programmer til elektronisk databehandling, eller i øvrigt at påvirke resultatet af en sådan databehandling, for eksempel ved gerningspersonens forsæt til at anvende de anskaffede oplysningerne til at foretage et online køb. Hvis oplysningerne eller programmerne anvendes, vil der være tale om fuldbyrdet databedrageri efter STRFL. § 279 a.

4.5.2 - Grænserne mellem straffelovens § 279 a, jf. § 21 og § 301

Herunder vil det analyseres, hvornår STRFL. § 301 og § 279 a, jf. § 21 vil benyttes efter den juridiske litteratur. Dernæst vil der fremhæves relevant retspraksis på området, for at kunne klarlægge både i hvilke tilfælde der dømmes efter STRFL. § 279 a, jf. § 21 i sammenstød med

²³¹ Betænkning nr. 1417, (København 2002), *Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet*, side 38.

²³² Betænkning nr. 1417, (København 2002), *Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet*, side 172 f

²³³ LFF.2003-11-05, nr. 55, punkt 15

²³⁴ Betænkning nr. 1417, (København 2002), *Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet*, side 173

STRFL. § 301, og i hvilke tilfælde der kun dømmes efter STRFL. § 301. Til sidst vil der kigges nærmere på dommene, for at analysere hvorfor der er blevet dømt som der er.

4.5.2.1 - Straf i sammenstød

For at belyse dette emne, vil der først blive gennemgået forskellige teoretiske holdninger til hvorvidt man bør straffe i sammenstød. Efterfølgende vil det undersøges hvilken holdning retspraksis understøtter.

Ifølge Lars Bo Langsted, kan der straffes efter STRFL. § 301 og § 279 a, jf. § 21 i sammenstød. For eksempel vil der i et tilfælde med opsætning af skimming udstyr, der benyttes til at kopiere magnetriben og aflure koden, for herefter at overføre dette til såkaldte ”hvide kort”, kunne straffes efter STRFL. § 301. Herefter bemærkes det, at der ikke bør straffes for forsøg på databedrageri i sammenstød med STRFL. § 301, medmindre gerningspersonen benytter disse kort til mislykkede forsøg på hævnninger, eller blive taget på fersk gerning i processen.²³⁵

Lasse Lund Madsen mener i modsætning til Lars Bo Langsted, at der ikke bør straffes i sammenstød ved STRFL. § 301 og § 279 a, jf. § 21. Han begrundet dette med henvisning til baggrunden for indførslen af STRFL. § 301, og denne sammenhæng med forsøgsansvaret. Lasse Lund Madsen lægger her vægt på, at der ved at straffe i sammenstød med § 279 a, jf. § 21 og § 301, vil kunne skabes en usikkerhed, i og med at forsættet til at bruge de anskaffede oplysninger skal konkretiseres, for at kunne benytte STRFL. § 279 a, jf. § 21. Han er af den opfattelse, at STRFL. § 301 kun skal anvendes hvis der ikke, eksempelvis ved skimming, er forsæt til konkret brug af de anskaffede oplysninger.²³⁶ Eftersom skimming ses at være forstadiet til databedrageri i STRFL. § 279 a, vil der ved et konkretiseret forsæt være tale om en fuldbyrdelse af forsøg på databedrageri.

4.5.3 - Retsspraksis vedrørende straffelovens § 279 a, jf. § 21, og § 301

Herunder vil der blive gennemgået relevant retspraksis, for at klarlægge hvorvidt den gældende ret på området tilgodeser Lasse Lund Madsens eller Lars Bo Langsteds ovenstående synspunkter, og for at undersøge grænserne mellem anvendelsen af STRFL. § 279 a, jf. § 21 og § 301.

TfK.2011.388.Ø

Denne dom omhandlede opsætning af skimmingudstyr ved en række hæveautomater i Danmark, for herefter at benytte de anskaffede oplysninger til fabrikering af falske betalingskort. Disse kort blev herefter anvendt i 1.118 tilfælde, til at hæve 1.881.200 kroner. Derudover blev disse forsøgt anvendt 2.913 gange, til at hæve 3.373.000 kroner. Der blev her udelukkende rejst tiltale for overtrædelse af STRFL. § 279 a, jf. 286, stk. 2 og forsøg herpå. Der blev altså ikke rejst tiltale for overtrædelse af STRFL. § 301, til trods for at gerningsindholdet herfor var fuldbyrdet. Domstolen tog ligeledes ikke stilling til, hvorvidt de tiltalte skulle straffes herfor.

²³⁵ Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48, side 4

²³⁶ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 7

Denne dom er et glimrende eksempel på Lasse Lund Madsens synspunkt, hvor der som nævnt ovenfor ikke skal straffes for STRFL. § 301, for så vidt der er tale om et fuldbyrdet forsøg på databedrageri.

AM.2013.03.18.B

I denne dom blev den tiltalte dømt efter STRFL. § 301, stk. 1, nr. 1, for at have opsat skimmingudstyr på en tankstation, til indhentning af oplysninger fra 72 betalingskort, der med forsæt skulle benyttes til uberettiget brug. Der tages i dommen ikke stilling til, hvorvidt den tiltalte skulle dømmes efter STRFL. § 279 a. Dette sker på den baggrund, at der må antages at være rejst tiltale for STRFL. § 279 a, i og med at der ikke i dommen benævnes, hvorvidt der kunne bevises et konkret forsæt til indgriben i elektronisk databehandling.²³⁷ Denne domsafsigelse er med til at understøtte Lars Bo Langsteds ovenstående synspunkt, hvorefter der ikke bør straffes for forsøg på databedrageri, medmindre gerningspersonen mislykket forsøger at benytte de indsamlede oplysninger, til enten hævnning af penge eller mislykket forsøger at benytte disse oplysninger til online køb.

TfK.2015.590.V og TfK.2016.464.V

Disse to domme viser situationer, hvor der er blevet straffet for henholdsvis STRFL. § 301, § 279 a, og § 279 a, jf. § 21. Dette sker på baggrund af, at gerningspersonerne i disse to sager var anklaget for, i flere tilfælde, at have opsat skimmingudstyr på tankstationer, med forsæt til uberettiget anvendelse, at have skaffet sig oplysninger som identificerer et betalingsmiddel. Efterfølgende oprettede gerningspersonerne i samarbejde med bagmænd falske betalingskort, som blev anvendt til, i flere tilfælde, henholdsvis at foretage hævnninger og mislykket forsøg på hævnninger. De mislykkede forsøg straffedes efter STRFL. § 279 a, jf. § 21, og de foretagne hævnninger straffedes efter STRFL. § 279 a.

Dommene viser at der straffes i sammenstød for STRFL. § 301, § 279 a, og § 279 a, jf. § 21, i og med at der efter STRFL. § 301 straffes for selve anskaffelsen, for herefter at straffe for såvel de mislykkede hævnninger som de faktiske hævnninger. Hermed understøttes Lars Bo Langsteds synspunkt yderligere, da der netop straffes i sammenstød til trods for, at der er sket et fuldbyrdet forsøg på databedrageri og fuldbyrdet databedrageri. Det ses da også i nyere retspraksis, at der straffes i sammenstød mellem STRFL. § 301 og § 279 a, jf. § 21.²³⁸

U.2023.1476 H

Der ses endvidere eksempler i den nyeste retspraksis, hvor der ligeledes bliver taget stilling til denne situation. I denne dom fra 2023, korrigerede byretten i Sønderborg tiltalen, således at der i stedet for at straffe efter STRFL. § 276, blev straffet efter STRFL. § 301, stk. 1, nr. 2. I dommen var situationen, at den tiltalte havde taget billeder af den forurettedes sygesikringskort

²³⁷ Se også U.2014.1241.V, hvor der ligeledes kun tiltales efter STRFL. § 301 og forsøg herpå, og hvor der heller ikke synes at være et konkret forsæt til uberettiget anvendelse af de anskaffede kortoplysninger

²³⁸ Ligeledes ses der at være straffet i sammenstød i TfK.2018.751.V, som her er med til at understrege at STRFL. § 301 ikke skal absorberes af STRFL. § 279 a, selvom databedrageribestemmelsen er fuldbyrdet

og dankort.²³⁹ Der kunne i denne sag dog ikke bevises et konkret forsæt til at udnytte disse oplysninger til uberettiget brug, hvorfor der ikke blev tiltalt efter STRFL. § 279 a, jf. § 21. Senere i dommen ses det dog, at Vestre Landsret igen korrigerede tiltalen, således at der straffedes efter STRFL. § 301, stk. 1, nr. 1, da oplysningerne der blev tilegnet, var fra et ægte betalingskort.

Denne dom er med til at vise, at der til stadighed findes tilfælde, hvor der kan være tvivl om hvornår der skal straffes efter STRFL. § 301, og herunder også hvornår stk. 1, nr. 1 og nr. 2 skal benyttes, den dag i dag.

4.5.4 - Opsummering

Efter behandling af de forhold der omhandler skimmingbestemmelsen i STRFL. § 301, ses der til stadighed at være en vis tvivl om hvornår der skal straffes efter STRFL. § 301, og i hvilke tilfælde der skal straffes efter STRFL. § 279 a, jf. § 21. Hertil er det dog ud fra ovenstående retspraksis gjort tydeligt at der, som også udtrykt af Lars Bo Langsted, skal straffes i sammenstød i de tilfælde, hvor der er tale om at der er benyttet et falsk betalingskort til, på fejlslagen vis, enten at hæve kontanter i en hæveautomat eller på anden vis er mislykket med brug af et falsk betalingskort.

Det er ligeledes gjort klart ud fra ovenstående, at der skal forelægge et konkret forsæt til at benytte de anskaffede oplysninger, til på uberettiget vis at opnå en vinding, førend der straffes for forsøg på databedrageri.

Dette konkrete forsæt foreligger, som det også kan ses i ovenstående gennemgang af retspraksis, som oftest i tilfælde hvor den tiltalte har fuldbyrdet databedrageribestemmelsen i STRFL. § 279 a. Eksempelvis hvis gerningspersonen hæver med et falsk betalingskort, for herefter også at have mislykkede forsøg på hævnninger. Hertil ses det, at dette konkrete forsæt findes i tilfælde, hvor der er tale om udlændinge der er rejst til Danmark med det ene formål at begå kriminalitet, idet de ikke har anden tilknytning til Danmark.

4.6 - Delkonklusion

I den ovenstående analyse og behandling af STRFL. § 279 a og de tilstødende bestemmelsers anvendelse i praksis, kan det konkluderes at der foreligger flere overlap mellem de forskellige bestemmelsers anvendelsesområder. Der vil herunder blive konkluderet på disse.

Straffelovens § 279 kontra § 279 a

Ovenstående kapitels analyse af retspraksis og den juridiske litteraturs synspunkt på området, har vist at både retspraksis og den juridiske litteratur har en fælles holdning, hvor afgrænsningen mellem STRFL. § 279 og STRFL. § 279 a findes i hvorvidt vildfarelseskravet er opfyldt.

²³⁹ U.2023.1476.H

Ligeledes er det observeret, at retspraksis først i dom TfK.2015.906.V foretog en egentlig stillingtagen til afgrænsningsspørgsmålet, og at der derfor før 2015 har været en uensartet praksis, for hvordan denne type forhold skulle afgøres. Denne dom fastlagde, at afgrænsningen mellem bedrageribestemmelsen i STRFL. § 279 og databedrageribestemmelsen i STRFL. § 279 a afhænger af, at en person der udfører en afprøvelse af de, af gerningspersonen afgivne oplysningers rigtighed, bliver vildledt.

Dette betyder, at anvendelsen af databedrageribestemmelsen i STRFL. § 279 a også kan komme på tale, selvom der er en person i den ordremodtagende virksomhed som behandler ordren efter instruks fra et automatiseret system, så længe personen blot følger instruksen og at den ansatte, grundet dennes lavere stilling, ikke afprøver korrektheden af de afgivne oplysninger.

Det kan derfor konkluderes, at der foreligger en klar afgrænsning mellem STRFL. § 279 og STRFL. § 279 a.

Straffelovens §278, stk. 1, nr. 3 og § 280 kontra § 279 a

Efter en gennemgående analyse af den retspraksis der foreligger på området, kan det observeres at der ikke foreligger en klar og ensartet praksis for hvornår der skal dømmes efter STRFL. § 279 a eller STRFL. § 278, stk. 1, nr. 3 og § 280.

Dommene der er blevet behandlet, omfatter i mange tilfælde ensartede forhold, men er ikke blevet afgjort efter samme bestemmelse. Om forholdet dømmes ud fra STRFL. § 279 a eller STRFL. § 278, stk. 1, nr. 3 og § 280 gør ikke afgørelsen mere eller mindre korrekt, da forholdene ofte kan falde ind under flere af bestemmelsesernes anvendelsesområder. Spørgsmålet om hvorvidt der skal rejses tiltale efter STRFL. § 279 a eller STRFL. § 278, stk. 1, nr. 3 og § 280 er derfor et spørgsmål om hvad anklageren i den pågældende sag finder mest korrekt.

Der kan derfor ikke udledes en konkret praksis på området, og spørgsmålet om hvor afgrænsningen mellem de tilstødende bestemmelser foreligger, må afklares på baggrund af den juridiske litteraturs meget sparsomme argumentation.

Som tidligere nævnt beskriver Straffelovrådet i betænkningen, at ved indførslen af databedrageribestemmelsen, vil de forhold som kan omfattes af STRFL. § 278, stk. 1, nr. 3 og § 280, men som indeholder elementer af elektronisk databehandling, blive omfattet af STRFL. § 279 a.

Straffelovrådet fastslår ikke at alle forhold der omfatter elektronisk databehandling vil skulle omfattes af databedrageribestemmelsen men blot henfører at der kan opstå situationer hvor databedrageribestemmelsen vil være mere korrekt at anvende. Herefter er det vurderet at Straffelovrådet ikke har ment at den elektroniske databehandling skal være en fast grænse for afgrænsningen mellem bestemmelserne, men at de forhold hvor anvendelsen af STRFL. § 278,

stk. 1, nr. 3 og § 280 vil skyldes en udvidelse af bestemmelsernes anvendelsesområder, vil være mere hensigtsmæssigt at afgøre efter STRFL. § 279 a.²⁴⁰

Straffelovens § 276 kontra § 279 a

Som tidligere nævnt, har der siden indførelsen af databedrageribestemmelsen længe hersket den opfattelse i tiltalepraksis, at tyveri af betalingskort med efterfølgende uberettigede hævnninger ved hæveautomater, var omfattet af tyveribestemmelsen i STRFL. § 276. Denne opfattelse var ligeledes understøttet af den daværende juridiske litteratur.

Først i 2014, ved dommen U.2014.1688.V, blev der endeligt taget stilling til afgrænsningsspørgsmålet mellem STRFL. § 276 og § 279 a. Siden da har der hersket en stort set ensartet praksis for, at selve borttagelsen af betalingskortet omfattes af tyveribestemmelsen i STRFL. § 276 og den uberettigede brug af betalingskortet, for at hæve penge ved en hæveautomat, omfattes af databedrageribestemmelsen i STRFL. § 279 a.

Dog har der været sager, hvor tiltalen ikke har fulgt den nye praksis, men faldet tilbage til den tidligere opfattelse af afgrænsningsspørgsmålet. Dette kan dog være grundet manglende kendskab til landsrettens afgørelse i U.2014.1688.V.

På nuværende tidspunkt følger retspraksis stadig den opfattelse, at forholdet skal opdeles i henholdsvis borttagelsen af betalingskortet, der omfattes af tyveribestemmelsen, og den uberettigede misbrug af betalingskortet, der omfattes af databedrageribestemmelsen.²⁴¹ Dog vurderes det på baggrund af den juridiske litteraturs argumentation, at der kan ske en subsumption af gerningsindholdet, men at det så vil være mere korrekt at henføre forholdet under databedrageribestemmelsen i STRFL. § 279 a.²⁴² Dette skyldes, at tyngden af gerningsindholdet ligger i den uberettigede brug af betalingskortet, og at den uberettigede tilegnelse af betalingskortet i første omgang nærmere må anses som værende en forberedende handling til databedrageriet.²⁴³ Dette er dog stadig blot en teoretisk stillingtagen, og ikke et synspunkt som retspraksis deler på nuværende tidspunkt.

Straffelovens § 280 kontra § 279 a

Afgrænsningen mellem anvendelsen af STRFL. § 279 a og § 280, ved forhold der omhandler misbrug af eget betalingskort, fastlægges ud fra den betalingsaftale der foreligger mellem Nets og den modtagende virksomhed.

Dette ses både i retspraksis og understøttes af den nuværende juridiske litteratur. Dog ses det kun i én af de behandlede domme, at der dømmes efter både mandatsvigsbestemmelsen og bedrageribestemmelsen i sammenstød med henvisning til garantigrænsen i betalingsaftalen.²⁴⁴ Den manglende stillingtagen skyldes, som tidligere nævnt, at alle de behandlede domme er

²⁴⁰ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 57-58

²⁴¹ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 7

²⁴² Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²⁴³ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²⁴⁴ AM.2012.02.16B3

blevet behandlet som tilståelsessager. Af den grund er det ikke fundet nødvendigt at afgøre afgrænsningsspørgsmålet.

Det konkluderes derfor, at der på nuværende tidspunkt foreligger en klar og korrekt retspraksis, angående afgrænsningen mellem STRFL. § 279 a og § 280.

Straffelovens § 301 kontra § 279 a

Grænsefladen mellem STRFL. § 279 a og § 301, ses at bero på konkretiseringskravet til gerningspersonens forsæt. Dette har den betydning, at det er nødvendigt at kunne bevise gerningspersonens forsæt til databedrageri, for at kunne dømme for forsøg på databedrageri. Hvis det nødvendige konkrete forsæt derimod ikke kan bevises, vil der kunne dømmes efter STRFL. § 301.

Hermed kan det altså udledes, at det er essentielt for Anklagemyndigheden at kunne bevise et konkret forsæt, for at kunne straffe for forsøg på databedrageri. Hvis dette ikke er muligt, vil det være vigtigt at få tiltalt efter STRFL. § 301 subsidiært.

Opsummering

Den ovenstående gennemgang og analyse viser, at der i nogle tilfælde ikke er en klar defineret afgrænsning mellem dele af de tilstødende bestemmelser. Det er særligt grænserne mellem STRFL. § 279 a og § 278, stk. 1 nr. 3, § 280 samt § 301 der som udgangspunkt ser ud til at være grænsegængerne.

Fælles for alle de ovenfor gennemgåede bestemmelser er, at det ikke umiddelbart er svært at skelne brugen af bestemmelserne fra hinanden, i tilfælde hvor der er tale om en klar overtrædelse af hver enkel bestemmelse individuelt. Problemerne med denne afgrænsning mellem bestemmelserne opstår, når der er tale om grænsetilfælde og overlapninger af hændelser og gerninger. Det er også især i disse situationer, at grænserne mellem STRFL. § 279 a og § 278, stk. 1 nr. 3, § 280 samt § 301 er vanskelige at definere. Som det ligeledes tidligere er nævnt, er det ikke kun i retspraksis denne udfordring ses, men også i den juridiske litteratur. Her syntes der heller ikke at være et klart skel mellem de pågældende bestemmelser. Netop denne afgrænsning mellem STRFL. § 279 a og de tilstødende bestemmelser er væsentlig og relevant at undersøge af flere årsager. Én af de vigtigste er, at der med en fast praksis for, hvornår et strafbart forhold falder ind under en given bestemmelse, kan dannes en ensartet retspraksis. Dette vil betyde, at alle kriminelle handlinger bliver straffet på samme måde som andre lignende kriminelle handlinger. Det gælder om at mindske tilfælde, hvor den kriminelle gerning falder mellem to eller flere bestemmelser, og det derfor vil være svært at straffe korrekt. For at søge for, at dette bliver mindsket, er det væsentligt at undersøge om retssystemet gør et aktivt forsøg på at ensrette retspraksis på området. Dette vil blive belyst nedenfor.

Kapitel 5 – Tiltalekorrektion

I det følgende afsnit vil det blive gennemgået, hvordan tiltalepraksis fungerer og herunder vil der sættes spørgsmålstejn ved praksisændringen, vedrørende det ovenfor nævnte skift der fandt sted i 2015.²⁴⁵

5.1 - Anklagemyndighedens opgaver

Det er Anklagemyndigheden der skal rejse tiltale mod den sigtede. Når der rejses tiltale, skal der udfærdiges et anklageskrift, som skal indeholde følgende;

”navnet på den ret, ved hvilken sagen anlægges, tiltaltes navn og adresse samt så vidt muligt personnummer el.lign. og oplysninger om det forhold, der rejses tiltale for.”²⁴⁶

Derudover skal oplysningerne om de forhold der rejses tiltale for, indeholde følgende;

”den regel, der påstås overtrådt, og forbrydelsens kendetegn, som de fremgår af reglen, forbrydelsens navn, hvis loven indeholder angivelse heraf, straffehjemmelen, en kort beskrivelse af det forhold, der rejses tiltale for, med sådan angivelse af tid, sted, genstand, udførelsesmåde og andre nærmere omstændigheder, som er nødvendig for en tilstrækkelig og tydelig beskrivelse, og i givet fald de strafforhøjelses- eller strafnedsættelsesgrunde, der vil blive påberåbt. jf. RPL §834, stk. 2., alternativ, herunder subsidier, tiltale er tilladt.”²⁴⁷

Det er som beskrevet ovenfor et krav, at der tages stilling til hvilken bestemmelse der tilsigtes at straffe efter og af den grund er det vigtigt, at det er den korrekte bestemmelse der er angivet i anklageskriftet.

Når et anklageskrift er udfærdiget, skal dette indleveres ved retten. Ved denne indlevering indledes straffesagen, jf. Retsplejelovens, herefter benævnt RPL., § 835, stk. 1. Efterfølgende skal der sendes en kopi til den tiltalte, som herefter straks skal forkyndes indholdet, jf. RPL. § 835, stk. 2. Slutligt skal der sendes en kopi af anklageskriftet til forsvareren så snart sagen er indledt, eller så snart en sådan er blevet beskikket den tiltalte, jf. RPL. § 835, stk. 3.

Efter anklageskriftet er udfærdiget og sendt ud, har Anklagemyndigheden den mulighed at de kan berigtige eller udvide tiltalen, helt indtil hovedforhandlingen. Efter hovedforhandlingens påbegyndelse vil det kræve rettens og den tiltaltes samtykke, at kunne udvide tiltalen i anklageskriftet. Det vil dog ikke kræve den tiltaltes samtykke, hvis der blot er tale om en berigtigelse af tiltalen.

I den tidligere nævnte dom, TfK.2015.443.Ø, ses et eksempel på hvorledes det kan foregå, når der anmodes om berigtigelse under en hovedforhandling. I denne dom afslog byretten

²⁴⁵ TfK.2015.906.V

²⁴⁶ Retsplejelovens § 834, stk. 1

²⁴⁷ Retsplejelovens § 834, stk. 3

anmodningen om berigtigelse fra STRFL. § 276 til § 279 a, med den begrundelse at det ville udvide tiltalen og dermed ville kræve samtykke fra de tiltalte. Anklagemyndigheden kærede byrettens beslutning, og landsretten tog kæremålet under påkendelse. Landsretten fastslog herefter at berigtigelsen blot ville ændre den citerede lovbestemmelse, og at der derfor ikke forelå en ændring af beskrivelsen af det strafbare gerningsindhold. Landsretten henviste i den forbindelse til U.2014.1688.V, i begrundelsen for godkendelsen af tiltaleændringen.

5.2 - Domstolenes behandling

Vigtigheden af, at Anklagemyndigheden på korrekt vis tager stilling til hvilken bestemmelse der tilsigtes at straffe efter, understreges. Faktum er, at dommere i sjældne tilfælde tager stilling til hvorvidt databedrageribestemmelsen skal benyttes frem for eksempelvis mandatsvigsbestemmelsen eller pengeunderslæbsbestemmelsen, hvis ikke Anklagemyndigheden sætter spørgsmålstegn ved dette.²⁴⁸

5.3 - Betydningen af berigtigelse eller udvidelse for tiltalte

Når der kigges på hvorvidt det har betydning for den tiltalte, om der dømmes efter eksempelvis mandatsvig, pengeunderslæb eller databedrageri, må det siges at have meget ringe betydning, da det formegentlig ikke vil have nogen indflydelse på strafudmålingen.

Hvis der tages et mere teoretisk blik på betydningen, kan det have en indflydelse på afgrænsningen mellem forsøg og fuldbyrdelse, hertil mulighederne for at dømme for medvirken.

I forlængelse heraf skal det faktum, at STRFL. § 279 a har et fremrykket fuldbyrdelsesmoment, hvorfor denne allerede er fuldbyrdet når den pågældende handling i forhold til it-systemet er foretaget, ligeledes nævnes. I sammenhæng med dette er det væsentligt at have for øje, at der i straffelovens berigelsesforbrydelsesbestemmelser findes et krav om risiko for formuetab. Dette krav har her ligeledes en større betydning for hvornår fuldbyrdelsestidspunktet finder sted. Altså vil der kunne straffes for en fuldbyrdet forbrydelse, i tilfælde hvor der eksempelvis i STRFL. § 278, stk. 1, nr. 3, ses at være en væsentlig risiko for formuetab, og hermed endnu ikke forelægger et reelt tab for den forurettede.²⁴⁹ Kravet om at det blot er nødvendigt, at der foreligger en væsentlig risiko for formuetab, kan altså også være med til at skabe en forskydning af netop fuldbyrdelsestidspunktet.

5.4 - Delkonklusion

I den ovenfor analyserede dom, TfK.2015.443.Ø, ses det, at retspraksis påvirker udviklingen af hvad der tilsigtes at dømme efter i anklageskriftet. Dette ses da der, som gennemgået ovenfor, helt frem til 2014, i sager omhandlende kontanthævninger ved brug af stjålne betalingskort, blev straffet for tyveri efter STRFL. § 276. Efter dommen i 2015, blev der dømt efter databedrageribestemmelsen, i STRFL. § 279 a. Dette er sket på trods af, at der i

²⁴⁸ Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 300

²⁴⁹ Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018, side 301

betænkningen, ved indførslen af STRFL. § 279 a i 1985, tydeligt udtrykkes at STRFL. § 276's benyttelse i sager der involverer data, vil være begrænset.

Til slut bemærkes det, at en berigtigelse eller udvidelse af anklageskriftet, kan have den betydning, at gerningspersoner i stedet for at blive straffet for forsøg på en af de tilstødende bestemmelser, kan ifalde strafansvar for fuldbyrdet databedrageri. Dette skyldes det fremrykkede fuldbyrdelsestidspunkt i STRFL. § 279 a.

Kapitel 6 – Hensigtsmæssig anvendelse?

I det følgende vil fokus blive rettet mod spørgsmålet, om hvorvidt STRFL. § 279 a anvendes i overensstemmelse med den hensigt, som bestemmelsen oprindeligt havde ved indførslen i 1985.

6.1 - Hensigtsmæssig anvendelse efter Straffelovrådets betænkning nr. 1032/1985?

Som tidligere gennemgået, ses det at STRFL. § 279 a er bredt formuleret. Dette ses i Straffelovrådets betænkning, følgende forklares;

”Med disse formuleringer undgår man at tage stilling til, om der umiddelbart ved indtastning af data eller lignende kan siges at være sket en databehandling, hvor et resultat er blevet påvirket, eller om dette først er tilfældet på et senere tidspunkt”²⁵⁰

Denne meget brede formulering har været med til, at bestemmelsen har kunnet benyttes på et meget bredt omfang af datakriminalitet, da den herved finder anvendelse på megen ny teknologi.

Den åbne formulering har ved indførelsen givet god mening. I 1985 var den teknologiske udvikling ikke nået nær så langt, som tilfældet er i dag. På trods af dette, havde man en evne til at se, at en sådan bestemmelse kunne blive nyttig i den nærmeste fremtid, med den teknologiske udvikling, der lå foran samfundet.

Som tidligere behandlet, har denne åbne formulering også været en af bestemmelsens svagheder. Dette har gjort, at den til tider ubestemmelige afgrænsning i et vist omfang, har været med til at gøre dens brug besværlig for flere aktører; først og fremmest for politiet og Anklagemyndigheden. Det kan ifølge Lasse Lund Madsen muligvis have spillet ind, at jurister ofte er et traditionsbundet folkefærd, og som han siger så er *”[g]amle vaner ikke er noget man slipper så let.”²⁵¹*

I specialets analyse, ses der at være et overlap mellem hvornår STRFL. § 279 a eller de tilstødende bestemmelser skal anvendes. Det bliver blandt andet beskrevet, at det er besværligt, ud fra retspraksis, at opsætte nogle konkrete grænser mellem hvornår STRFL. § 279 a kontra § 278, stk. 1, nr. 3 og § 280 skal anvendes. Dette overlap er et tydeligt tegn på, at det til stadighed ikke falder naturligt for hverken anklagere eller dommere, at alle tilfælde der involverer data skal henføres under STRFL. § 279 a, som det beskrives at være hensigten i Straffelovrådets betænkning.

6.2 - Fremrykket fuldbyrdelsesmoment

Baseret på ovenstående, hvor det ses hvordan tiltale- og retspraksis ikke er ensrettet, med hensyn til overtrædelse af STRFL. § 279 a, jf. § 21, og § 301, udledes det at der for at straffe

²⁵⁰ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 82

²⁵¹ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 2

efter STRFL. § 279 a, jf. § 21, kræves et konkret forsæt til at ville begå databedrageri. Hvis dette ikke kan bevises, vil der straffes efter STRFL. § 301. Denne bestemmelse er skabt til at dække de tilfælde, der falder før STRFL. § 279 a, hvorfor der netop dannes en svær bedømmelse mellem benyttelsen af § 279 a, jf. § 21 og § 301. I betænkningen fra 2002 ligger udvalget også vægt på, at falske betalingskort ofte er et organiseret kriminalitetsområde, hvor der opereres i flere lande samtidigt.²⁵² Netop herfor mener udvalget, at der er et behov for at kunne straffe for produktion, anskaffelse og besiddelse, med forsæt til at anvende kortene som ægte og videregive disse falske kort, uagtet om forsøgsforsæt kan bevises.²⁵³

Straffelovrådets begrundelse for nødvendigheden af et fremrykket fuldbyrdelsesmoment, er at det er vanskeligt, for ikke at sige umuligt, at kunne fastsætte et bestemt tidspunkt hvor den ændrede oplysning er blevet anvendt.²⁵⁴ Der må dog argumenteres for, at det i dag ved hjælp af digitale log systemer, er muligt at følge, hvornår den pågældende ændrede oplysning anvendes. Herfor udledes det, at dette fremrykkede fuldbyrdelsesmoment, givetvis ikke har sit fæste i nutidens udviklede digitale samfund.

Lasse Lund Madsen udtaler i denne forbindelse følgende;

*”Typisk vil det retsstridige misbrug, der har ført til et formuetab, afsætte elektroniske spor, der – i hvert fald i dag – ofte lader sig tidsfæste relativt præcist.”*²⁵⁵

Her understøttes ovenstående udtalelse netop. Således bør der stilles spørgsmålstegn, ved hvorvidt dette fremrykkede fuldbyrdelsesmoment er hensigtsmæssigt i nutidens digitale virkelighed.

Lasse Lund Madsen stiller sig, i sin artikel *“Bedrageri i den digitale virkelighed”*, også her spørgende overfor, hvorvidt fuldbyrdelsesmomentet for STRFL. § 279 a ikke burde ligestilles med de resterende berigelsesforbrydelser, således at forbrydelsen først fuldbyrdes ved formuetab eller risiko herfor.²⁵⁶

²⁵² TfK.2015.590.V

²⁵³ Betænkning nr. 1417, (København 2002), *Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet*

²⁵⁴ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 82

²⁵⁵ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 3

²⁵⁶ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 3

Kapitel 7 - Perspektivering

7.1 - Indledende bemærkninger

Igennem denne afhandlings analyse, henviser såvel betænkningen som den juridiske litteratur til hvordan man har valgt at håndtere de problematikker vedrørende datakriminalitet der måtte opstå ved internettets udbredelse. Disse henvisninger har, af relevans for afhandlingens emne, skabt en interesse for at dykke ned i den nordiske behandling af disse problemstillinger.

I Straffelovrådets betænkning fra 1985, foretages der et indblik i, hvordan man i Norge, Sverige og Finland behandlede datarelateret kriminalitet på daværende tidspunkt.²⁵⁷ Hertil henviser blandt andre Lasse Lund Madsen også til den nordiske behandling af den datarelaterede problematik.²⁵⁸

I denne forbindelse er det valgt at analysere den norske, svenske og finske tilgang til formueforbrydelsernes digitale udvikling, samt OECD's anbefaling på det daværende tidspunkt. Dette udføres for at give et overblik over, hvordan vores nabolande har valgt at behandle disse former for datarelaterede berigelsesforbrydelser. På baggrund af dette overblik, vil der til slut i dette kapitel opsummeres, hvorledes gældende ret foreligger.

7.2 - Straffelovrådets bemærkninger i betænkning nr. 1032/1985

Med henblik på bedrageri, nævner Straffelovrådet i deres betænkning, at Norge kriminaliserer bedrageri således;

*”at gerningsmanden »ved å framkalle, styrke eller utnytte en villfarelse rettsstridig forleder noen til en handling, som volder tap eller fare for tap for ham eller den han handler for.« ”*²⁵⁹

I 1983 skete det ligeledes, at det norske straffelovsråd fik til opgave at undersøge, hvorvidt den norske straffelov var dækkende med hensyn til datakriminalitet. Hertil skriver det danske Straffelovråd, at man forventede at der ville komme en ny norsk betænkning i 1985.²⁶⁰ Dette betyder, at der ved den danske behandling af hvorvidt der på datakriminalitetsområdet var nogle mangler i den danske straffelov, havde det norske Straffelovråd endnu ikke fået udarbejdet og offentliggjort deres betænkning. Af denne grund kunne man se til den dagældende norske ret.

Danmarks indførsel af databedrageribestemmelsen i 1985 var, trods dens relative tidlige indførsel, ikke den eneste indførsel af en form for straffebestemmelse angående databedrageri. I de andre nordiske lande fandt man det, samtidig med Danmark, ligeledes nødvendigt med indførslen af databedrageribestemmelser.²⁶¹

²⁵⁷ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 6

²⁵⁸ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²⁵⁹ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 49

²⁶⁰ Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*, side 6

²⁶¹ SFS 1986:123 og NOU 1985:31

7.3 - Det norske Straffelovråds betænkning NOU 1985:31

Man har i NOU 1985:31, vedrørende det norske Straffelovråds analyse af gældende ret, og hvorvidt der er behov for ændringer i denne henseende, kigget mod andre lande som Sverige, Finland, Vest-Tyskland, Danmark, USA og Canada. Det norske Straffelovråd har her forsøgt at finde ud af, hvad andre lande har fremlagt på området for datakriminalitet.²⁶²

I den norske betænkning der, som tidligere nævnt, ligger til grund for indførslen af den norske straffebestemmelse om databedrageri, er der blevet argumenteret for, at selvom kun en mindre del af straffebestemmelserne er udformet med henblik på at indeholde handlinger udført i dataforhold, vil de fleste straffebestemmelser kunne rumme dataforhold ved en rimelig fortolkning af disse straffebestemmelser;

”Det er likevel grunn til å tro at de fleste av de mest praktiske former for slik kriminalitet er dekket av gjerningsbeskrivelsene i gjeldende bestemmelser, ved en rimelig tolking av disse. Blant de straffebestemmelser som særlig kan være aktuelle kan nevnes straffelovens § 145 (som blant annet dekker inntrenging i datasystemer), straffelovens § 255 (underslag), straffelovens § 257 (tyveri), straffelovens § 270 (bedrageri), straffeloven § 275 (utroskap)...”²⁶³

Det norske Straffelovråd fastslår dog videre at;

”Det er likevel grunn til å tro at visse typer straffverdige handlinger innen dette området ikke vil dekkes av noen eksisterende straffebestemmelser, eller at det iallfall kan være behov for en klargjøring, der også straffesatsene blir overveid.”²⁶⁴

Her fastslår det norske Straffelovråd, ligesom det danske, at der kan forekomme situationer hvor den kriminelle handling ikke kan indeholdes af de traditionelle straffebestemmelseres gerningsbeskrivelser.²⁶⁵ Denne holdning bliver efterfølgende understøttet af regeringens svar på en anmodning af stortingsrepræsentanten, Morten Steenstrup, der i 1982 havde fremført spørgsmålet, om den norske regering kunne foretage en redegørelse over de forskellige former for datakriminalitet i straffeloven.

Her blev det fremført, at mere og mere kriminalitet var blevet digital, men kun et mindre antal af datakriminaliteten blev egentlig opdaget og et endnu mindre antal blev anmeldt;

”Mye tyder på at en forholdsvis liten andel av handlingene innenfor området datakriminalitet fører til noen strafferettslig reaksjon, kanskje særlig i tilfelle hvor den straffbare handling er rettet mot EDB-utstyr eller programmer. I en rapport fra det amerikanske handelsdepartement er det anslått at det i USA er ca 100 uoppdagede kriminelle handlinger for hver som blir oppdaget på dette området, og at bare en av fem av de oppdagede

²⁶² NOU 1985:31, side 21-26

²⁶³ NOU 1985:31, side 5

²⁶⁴ NOU 1985:31, side 5

²⁶⁵ NOU 1985:31, side 5

forbrytelsene blir anmeldt. Selv om man ikke har holdepunkter for å anta at anslag fra andre land kan anvendes på kriminalitetsbildet Norge, ser jeg ikke bort fra at slik kriminalitet kan ha et visst omfang også hos oss.”²⁶⁶

Selvom det var konkluderet, at der var behov for en indførsel af straffebestemmelser angående datakriminalitet, fandt det norske Straffelovråd det dog unødvendigt at lade en databedrageribestemmelse omfatte tilfælde, hvor der forelå uberettigede hævnninger i pengeautomater;

”Straffelovrådet antar at subsumsjon under tyveriparagrafen fremdeles vil være det naturlige ved manipulasjoner som direkte overfører besittelsen av penger eller andre ting til gjerningsmannen, selv om gjerningsbeskrivelsen i § 270 nr. 2 i og for seg også dekker slike tilfelle.”²⁶⁷

Herefter lægges der vægt på, at der ved tilfælde om hævnninger i automater, dette værende om de fungerer mekanisk eller om datamekanikken er taget i brug, stadig fremadrettet vil falde under tyveribestemmelsen, til trods for at gerningsindholdet også vil høre under den nye stk. 1, nr. 2 i § 270.²⁶⁸

Yderligere vurderedes det, at der er en sådan lighed med bedrageribestemmelsen, at tilføjelsen om databedrageri indføres som en del af bedrageribestemmelsens stk. 1, nr. 2. Der kommenteres her også på de tilfælde, hvor en gerningsperson, ved at indtaste urigtige oplysninger direkte ind i en datamat, for at føre en person bag lyset og lede dem til en tabsbringende disposition. Her vil disse tilfælde under gældende ret falde under tyveri, - eller underslæbsbestemmelsen. Dog vil det ses som værende tvivlsomt, om hvorvidt forbrydelsen efter gældende ret i 1985 ville være fuldbyrdet før end gerningspersonen havde tilegnet sig beløbet. I modsætning hertil, vil forbrydelsen, efter den nye databedrageribestemmelse, være fuldbyrdet allerede når risikoen for tab er forvoldt, hvilket normalt vil sige så snart de urigtige data er indtastet.

Først ved ikrafttræden af Ot.prp. nr. 22 (2008-2009), blev der tilføjet en udvidelse af databedrageribestemmelsens beskrivelse, Denne præciserede at kriminelle handlinger, hvor gerningspersonen misbrugte en ham givet adgang til en andens betalingskort, for at foretage varekøb eller overføre penge til egen konto fra den forurettedes konto, ligeledes ville være omfattet.²⁶⁹ Dog blev det fastslået, at et misbrug af en andens betalingskort for efterfølgende at foretage hævnninger i en pengeautomat, forsat ville være omfattet af tyveribestemmelsen;

”Misbruk av bankkort til direkte uttak, skal derimot som i dag straffes som tyveri, jf. Ot.prp. nr. 35 (1986 - 87) side 26.”²⁷⁰

²⁶⁶ NOU 1985:31, side 5

²⁶⁷ NOU 1985:31, side 33

²⁶⁸ NOU 1985:31, side 33

²⁶⁹ Ot.prp., nr. 22, 2008-2009, side 464

²⁷⁰ Ot.prp., nr. 22, 2008-2009, side 464

Der hersker derfor ikke nogen tvivl i den norske strafferet, om at uberettigede hævnninger fortsat er omfattet af tyveribestemmelsen og dermed ikke er omfattet af den nuværende norske straffelovs § 371, bokstav b.²⁷¹

7.4 - Det svenske synspunkt

I Sverige er der blevet udarbejdet en databedrageribestemmelse baseret på en lex specialis-betragtning, hvilket medførte indførslen af 9:1 Brottsbalken (BrB), stk. 2;

“För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan.”²⁷²

Misbrug af kort ved pengeautomater skulle derfor herefter ikke bedømmes efter den svenske tyveribestemmelse, som ellers tidligere var praksis, men derimod omfattes af den, på det pågældende tidspunkt, nyindførte databedrageribestemmelse.²⁷³ I en kommentar til Brottsbalken udtrykkes det således;

”[s]ådana fall bör numera bedömas enligt 9:1 andra stycket BrB, da denne bestämmelse har karaktären av en specialregulering.”²⁷⁴

7.5 - Finsk løsning af afgrænsningsproblematikken

I 1980 oprettede det finske justitsdepartement en komité, til at udarbejde udkast til en ny straffelov, hvor der var taget højde for datateknologiens udvikling og dennes påvirkning på kriminaliteten. Komitéen fandt, at særligt angående formueforbrydelser der involverede dataforhold, var det nødvendigt med en revidering af den daværende straffelov.²⁷⁵ I 1984 udlagde de et udkast til flere straffebestemmelser, som var ment til at kunne omfatte datakriminalitet.

En af disse straffebestemmelser omfattede databedrageri der, efter en nyaffattelse i 2003, har følgende ordlyd;

“För bedrägeri döms också den som i sådant syfte som nämns i 1 mom. matar in, ändrar, förstör eller undertrycker data eller på något annat sätt ingriper i ett informationssystems funktion så att resultatet av databehandlingen förvanskas och därigenom orsakar ekonomisk skada för någon annan.”^{276 277}

²⁷¹ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²⁷² 9:1, Brottsbalken (BrB), stk. 2

²⁷³ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5 og SFS 1986:123

²⁷⁴ Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343, side 5

²⁷⁵ NOU 1985:31, side 23

²⁷⁶ NOU 1985:31, side 23-24

²⁷⁷ Strafflag (39/1889), kap. 36, § 1, stk. 2

Her ses det foreskrevet, at en uberettiget påvirkning af en databehandling, hvorved et tab realiseres, kriminaliseres.

Udover denne bestemmelse forelagde komitéen et udkast til en straffebestemmelse, omhandlende betalingsmiddelsbedrageri.²⁷⁸ Efter en nyaffattelse i 2021, har denne bestemmelse følgende ordlyd;

”Den som för att bereda sig eller någon annan orättmätig ekonomisk vinning
1) använder ett betalningsmedel utan tillstånd av dess lagliga innehavare, med överskridande
av den rätt tillståndet ger honom eller henne eller annars utan laglig rätt,
2) använder ett falskt eller förfalskat betalningsmedel, eller
3) matar in, ändrar, förstör, skadar, överför eller raderar data i anslutning till ett
betalningsmedel eller på något annat sätt ingriper i ett informationssystems funktion så att
resultatet av överföring av pengar eller penningvärde förvanskas och därigenom orsakar
någon annan en ekonomisk skada...
...För betalningsmedelsbedrägeri döms också den som genom att överskrida täckningen på
ett konto eller en avtalad högsta kreditgräns missbrukar ett betalningsmedel som avses i 1
mom. och därigenom orsakar någon annan en ekonomisk skada, om inte han eller hon vid
*användningen av betalningsmedlet hade för avsikt att utan dröjsmål ersätta skadan...”*²⁷⁹

Denne bestemmelse kan ses at omfatte forskellige situationer, omfattende misbrug af betalingsmidler. I bestemmelsens stk. 1, nr. 1 omfattes de situationer, hvor en person misbruger en adgang til en anden persons betalingsmiddel uden dennes samtykke, eller ved overskridelse af et givent samtykke.²⁸⁰

Stk. 1, nr. 2 omfatter de tilfælde hvor en gerningsperson benytter et falskt betalingsmiddel.²⁸¹

Bestemmelsens stk. 1, nr. 3 omfatter forhold, hvor der foretages en tilføjelse, ændring, ødelæggelse, skade eller sletning af data i forbindelse med et betalingsmiddel. Ligeledes omfatter bestemmelsen indgreb i et datasystem, så overførsel af penge eller værdien af pengene formindskes, og dermed medfører den forurettede et tab.²⁸²

Dertil foreskriver bestemmelsens stk. 2, at overskridelsen af dækning på en konto eller overskridelsen af en allerede aftalt kreditgrænse, ligeledes omfattes af betalingsmiddelbedrageribestemmelsen, medmindre gerningspersonen havde til hensigt at erstatte skaden, og at dette gøres uden ophold.²⁸³

²⁷⁸ NOU 1985: 31, side 24

²⁷⁹ Strafflag (39/1889), kap. 37, § 8

²⁸⁰ Strafflag (39/1889), kap. 37, § 8, stk. 1, nr. 1

²⁸¹ Strafflag (39/1889), kap. 37, § 8, stk. 1, nr. 2

²⁸² Strafflag (39/1889), kap. 37, § 8, stk. 1, nr. 3

²⁸³ Strafflag (39/1889), kap. 37, § 8, stk. 2

7.6 - OECD's anbefalinger og guidelines

I 1983 blev der nedsat en ekspertgruppe ved OECD, der inkluderede repræsentanter fra flere af medlemslandene, herunder repræsentanter fra England, Frankrig og Norge. Formålet var at vurdere mulige manglende internationale tiltag, angående datakriminalitet. Ekspertgruppen anbefalede, at der blev udarbejdet en rapport for at kunne fastlægge en vurdering som medlemslandene kunne benytte, med henblik på medlemslandets egen straffelovgivning angående datakriminalitet.²⁸⁴

I 1986 udgav OECD rapporten 'Computer-related Criminality; Analysis of Legal Policy in the OECD Area', der oplyste følgende handlinger af datakriminalitet som kunne forekomme;

- “- The input, Alteration, erasure and/or supression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;*
- The input, Alteration, erasure and/or supression of computer data and/or computer programs made wilfully with the intent to commit a forgery;*
- The input, Alteration, erasure and/or supression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunications system... ”²⁸⁵*

Rapportens analyse fastslår, at disse typer af kriminelle handlinger ville være problematiske at få omfattet af de traditionelle straffebestemmelser, ligesom disse handlinger i større grad ville kunne overskride landegrænser og dermed kræve større internationalt samarbejde.²⁸⁶ Videre anfører OECD's rapport mulige tilgange til at løse anvendelsesproblematikken ved digitale kriminelle handlinger, herunder muligheden for at indføre supplerende straffebestemmelser eller adaptere allerede eksisterende straffebestemmelser, til at omfatte handlinger udført i dataforhold.²⁸⁷

7.7 - Opsummering

Mellem 1980 og 1990 sås det, blandt flere af de nordiske lande og blandt internationale organisationer, at være nødvendigt at tage stilling til den voksende udvikling angående datarelateret kriminalitet. Den Europæiske Komité for Kriminelle Problemer udtrykte det således i 1990;

“The new technology has brought a great many benefits to government and business administration and to the citizen himself... ..It can also be used to commit (or simplify the commision of) classical crimes, such as theft and fraud. ”²⁸⁸

²⁸⁴ NOU 1985:31, side 27

²⁸⁵ European Committee on Crime Problems, Computer-related Crime, 1990, side 10
Landsted

²⁸⁶ European Committee on Crime Problems, Computer-related Crime, 1990, side 20

²⁸⁷ European Committee on Crime Problems, Computer-related Crime, 1990, side 20

²⁸⁸ European Committee on Crime Problems, Computer-related Crime, 1990, side 12-13

De nordiske lande har dog haft forskellige tilgange til at imødekomme denne digitale udvikling. I Norge har man valgt at tage det synspunkt, at flere af de eksisterende straffebestemmelser i den norske straffelov kan omfatte det digitale aspekt af de traditionelle straffebestemmelser. Dog tilkendegiver de også, at der kan opstå situationer der ikke kan indeholdes af traditionelle bestemmelser, og dermed kræver en selvstændig bestemmelse. I Norge er den uberettigede hævnning ved pengeautomater fortsat omfattet af den norske tyveribestemmelse.

I Sverige har man betragtet den svenske databedrageribestemmelse som speciallovgivning og ser derfor, at den uberettigede brug af betalingskort ved pengeautomater skal omfattes af en databedrageribestemmelse.

I Finland er der blandt andet blevet indført en databedrageribestemmelse. Derudover har Finland også set det nødvendigt at indføre en særskilt bestemmelse omhandlende misbrug af betalingsmidler, og om hvorvidt dette er gerningspersonens eget betalingsmiddel, om det er et falsk betalingsmiddel eller om det er stjålet.

Selvom disse tilgange varierer fra hinanden, imødekom de alle den problemstilling som blev fremført i OECD's rapport. Nemlig nødvendigheden af at revurdere de traditionelle bestemmelser, med tanke på den digitale udvikling.

Kapitel 8 - Konklusion

Efter afhandlingens analyse af relevant retspraksis, i forbindelse med STRFL. § 279 a samt de tilstødende bestemmelser, sammenholdt med den gennemgåede juridiske litteratur, kan det først og fremmest konkluderes, at STRFL. § 279 a siden 1985 har fået et udvidet anvendelsesområde.

Fra databedrageribestemmelsens indførelse i 1985 til henholdsvis 2014 og 2015, fandtes der at være tvivl angående hvornår STRFL. § 279 a skulle anvendes, og på hvilke tilfælde. Dette er blevet vist igennem afhandlingen, ved hjælp af relevant retspraksis. I 2014 ses det, at dommen U.2014.1688.V havde en skelsættende betydning, da den tog stilling til hvornår der skal dømmes for databedrageribestemmelsen i STRFL. § 279 a, i forhold til hvornår der skal dømmes efter tyveribestemmelsen i STRFL. § 276 – selvfølgelig kun i situationer der ligner dommens faktum.

I 2015 blev dommen TfK.2015.906.V skelsættende, da den tog stilling til hvornår der er tale om henholdsvis bedrageri i STRFL. § 279 eller databedrageri i STRFL. § 279 a, i forbindelse med online transaktioner. Der ses dog til stadighed at opstå tvivlstilfælde om hvornår STRFL. § 279 a eller en af de tilstødende bestemmelser som nævnt ovenfor, skal benyttes. Herfor kan det konkluderes, at den brede udformning databedrageribestemmelsen fik i 1985, har gjort at den stadig kan benyttes i mange tilfælde i dag, til trods for at det ikke endnu er helt fastlagt, hvilke tilfælde der skal kategoriseres under STRFL. § 279 a eller de tilstødende bestemmelser.

Baseret på ovenstående, kan det konkluderes, at den brede formulering som databedrageribestemmelsen fik tilbage i 1985, har været med til at den har kunnet følge udviklingen i det mere og mere dataprægede samfund, der stadig ses at udvikle sig. Dette har medført, at bestemmelsens anvendelsesområde gennem tiden siden 1985, er blevet udvidet.

Derudover viser afhandlingens grundige analyse af både litteratur og retspraksis, interessante perspektiver i forhold til afgrænsningen mellem STRFL. § 279 a og de tilstødende bestemmelser. Det kan konkluderes, at der er en klar afgrænsning mellem STRFL. § 279 a og § 276 om tyveri og § 279 om bedrageri. Dette er især med udgangspunkt i ovenstående afsnit, hvor henholdsvis U.2014.1688.V og TfK.2015.906.V er inddraget.

I forhold til afgrænsningen mellem forsøg på databedrageri efter STRFL. § 279 a og § 301 om skimming, er retspraksis en smule uklar. Dette skyldes udfordringen i at fastlægge, hvornår den kriminelle handling går fra at være henholdsvis det ene eller det andet. Det kan dog ud fra forarbejderne konkluderes, at denne væsentlige forskel bunder i, at gerningspersonen skal have forset, som er tilstrækkeligt konkret i den pågældende situation, for at gerningspersonen kan dømmes efter STRFL. § 279 a, jf. § 21.

Videre kan det konkluderes, at retspraksis ikke har taget afgørende stilling til, hvor afgrænsningen mellem STRFL. § 279 a og § 278, stk. 1, nr. 3 og § 280 skal gå. Valget om hvorvidt det er STRFL. § 279 a om databedrageri, § 278, stk. 1 nr. 3 om pengeunderslæb eller

§ 280 om mandatsvig der skal rejes tiltale efter, kan med fordel tage udgangspunkt i det følgende.

Sondringen mellem hvilken af de tre bestemmelser der skal anvendes, bør træffes med udgangspunkt i hvilken metode gerningspersonen bruger, til at opnå den pågældende berigelse. Derfor vurderes det, at i en situation hvor gerningspersonen har lavet et indgreb i en elektronisk databehandling og har et forsæt til berigelse, så findes det mest hensigtsmæssigt at der rejses tiltale og dømmes efter databedrageribestemmelsen i STRFL. § 279 a. I en situation hvor der foreligger et ansættelsesforhold mellem gerningspersonen og den forurettede, vil det bero på en konkret vurdering, hvorvidt det findes mest korrekt at rejse tiltale og dømme efter STRFL. § 278, stk. 1, nr. 3, § 280 eller § 279 a.

Overordnet set må det konkluderes, at det i praksis er af mindre betydning, om der dømmes efter STRFL. § 279 a eller en af de tilstødende straffebestemmelser. Grunden hertil er, at både STRFL. § 279 a og de tilstødende straffebestemmelser der er blevet behandlet i denne afhandling, har samme strafferamme. Derimod foreligger der en teoretisk betydning for afgrænsningen mellem fuldbyrdelse, forsøg og medvirken, om hvorvidt der rejses tiltale efter STRFL. § 279 a eller en tilstødende bestemmelse.

Databedrageribestemmelsen indeholder et fremrykket fuldbyrdelsesmoment, hvilket vil resultere i at den tiltalte dømmes for en fuldbyrdet kriminaliseret handling tidligere, end hvis der i stedet var rejst tiltale efter en af de tilstødende straffebestemmelser. Kernen af denne problemstilling ligger i, at hvor der i nogle tilfælde ville være dømt for forsøg eller medvirken til en af de tilstødende straffebestemmelser som eksempelvis underslæb, også ville kunne dømmes efter fuldbyrdet databedrageri hvis STRFL. § 279 a i stedet bruges ved tiltalerejsningen.

Den meget åbne formulering i STRFL. § 279 a, medfører en bred anvendelse på forskellige former for datakriminalitet. Dette er både positivt, da bestemmelsen kan indeholde den teknologiske udvikling der er sket siden bestemmelses indførelse i 1985, men også negativt da det stiller spørgsmål ved afgrænsning mellem databedrageribestemmelsen og de tilstødende bestemmelser, herunder særligt STRFL. § 278, stk. 1, nr. 3 og § 280. Udover databedrageribestemmelsens åbne formulering, medfører den stigende digitalisering af eksempelvis pengesystemer, at mere kriminalitet foregår digitalt. Her bliver spørgsmålet mere og mere relevant, om hvorvidt brugen af underslæbsbestemmelsen bliver overflødig, hvis den ikke kan finde anvendelse ved handlinger udført i et digitalt perspektiv.

Det kan ligeledes konkluderes, at der foreligger en problemstilling vedrørende det fremrykkede fuldbyrdelsesmoment ved databedrageribestemmelsen. Dette gælder både mellem fuldbyrdet databedrageri og forsøg på en af de tilstødende straffebestemmelser, men også mellem forsøg på databedrageri og fuldbyrdet overtrædelse af STRFL. § 301.

Dette fremrykkede fuldbyrdelsesmoment havde tidligere en nødvendighed i og med, at teknologien på det pågældende tidspunkt ikke kunne udføre en tidsfastsættelse af

databehandlingen. I dag må det konkluderes, at der ikke længere foreligger en nødvendighed af det fremrykkede fuldbyrdelsesmoment, da man med tidens teknologi har mulighed for at tidsfastsætte samtlige elektroniske databehandlinger, med forholdsvis præcis nøjagtighed. Her udtrykker den juridiske litteratur at det bør tages op til overvejelse, hvorvidt fuldbyrdelsesmomentet i STRFL. § 279 a bør ligestilles med de tilstødende bestemmelser.

Afslutningsvist kan det, for denne kandidatafhandling konkluderes, at det strafferetlige værn mod digital berigelseskriminalitet og databedrageri er tilstrækkeligt dækkende. Der forelægger dog teoretiske problemstillinger i forbindelse med afgrænsningen mellem STRFL. § 279 a og de tilstødende bestemmelser, grundet databedrageribestemmelsens brede formulering.

Litteraturliste

Juridisk litteratur

Carsten Munk-Hansen, *Den juridiske løsning: Introduktion til den juridiske metode*, (København: jurist- og økonomforbundets forlag, 2017)

Gorm Toftegaard Nielsen, *Om at lære strafferet og/eller begreber*, U.1990B.329

Gorm Toftegaard Nielsen, Thomas Elholm og Morten Niels Jakobsen, *Kommenteret straffelov – Speciel del*, (København: jurist- og økonomforbundets forlag, 2017)

Jens Røn, *Databedrageri – stadig en overset bestemmelse?*, Festskrift til Lars Bo Langsted, 2018

Knud Waaben, *Strafferettens almindelig del*, (København: Karnov Group, 2015)

Knud Waaben, *Strafferettens almindelige del I – Ansvarslæren*, (København: Karnov Group, 2015)

Knud Waaben, *Strafferettens specielle del*, (København: Karnov Group, 2014)

Lars Bo Langsted, *Dankortet i strafferetlig belysning*, U.2019B.48

Lars Bo Langsted og Peter Helbo Langsted, *Hovedlinjer i erhvervsstrafferetten*, (København: DJØF forlag, 2020)

Lasse Lund Madsen, *Bedrageri i den digitale virkelighed*, U.2016B.343

Mads Bryde Andersen, *IT-retten*, (København: Gjøellerup, 2005)

Peter Blume, *Retssystemet og juridisk metode*, (København: jurist- og økonomforbundets forlag, 2016)

Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, *Kommenteret Straffelov – Speciel Del*, (København: jurist- og økonomforbundets forlag, 2022)

Vagn Greve, Poul Dahl Jensen og Gorm Toftegaard Nielsen, *Kommenteret Straffelov – Speciel del*, (København: jurist- og økonomforbundets forlag, 2012)

Lovgivning, lovforslag mm.

LBKG. 2022-09-28, nr. 1360

LFF.1985-04-24

LFF.2003-11-05

NOU 1985:31

Ot.prp., nr. 22, 2008-2009

Retsplejeloven

SFS 1986:123

Straffeloven

Strafflag (39/1889)

9:1, Brottsbalken (BrB)

Internetsider

<https://badv.dk/faq/hvad-er-databedrageri/> - Hvad er databedrageri?

<https://dejuridiskemetoder.digi.hansreitzel.dk/?id=222> – De juridiske metoder

<https://denstoredanske.lex.dk/berigelsesforbrydelser> - Berigelsesforbrydelser

<https://denstoredanske.lex.dk/Nets> - Nets

<https://digital-strategy.ec.europa.eu/en/policies/desi> - The Digital Economy and Society Index (DESI)

<https://politi.dk/syddjyllands-politi/nyhedsliste/22-aarig-mand-doemt-for-trickyveri-og-databedrageri-af-aeldre-kvinder/2022/01/14> - 22-årig mand dømt for trickyveri og databedrageri af ældre kvinder

<https://politiken.dk/indland/art9196874/Flere-anmelder-bedrageri-til-politiet---særligt-databedrageri-fylder> - Flere anmelder bedrageri til politiet – særligt databedrageri fylder

<https://www.altinget.dk/digital/artikel/marie-bjerre-om-digital-brydningstid-mere-og-hurtigere-er-ikke-laengere-maalet-nu-handler-det-om-den-rigtige-digitalisering> - Hun er

Danmarks første minister på området: Mere og hurtigere er ikke længere målet, nu handler det om den rigtige digitalisering

<https://www.berlingske.dk/dine-penge/forskere-spaar-kontantloest-danmark-i-2025> —

Forskere spår kontantløst Danmark i 2025

<https://www.dankort.dk/dk/om-dankort/> - Fakta om Dankort

<https://www.domstol.dk/vestrelandsret/aktuelt/2022/12/3-8-aars-faengsel-for-saerlig-grove-databedragerier-ved-nemid-svindel/> - 3-8 års fængsel for særlig grove databedragerier ved NemID-svindel

<https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=40257> — Fortsat stigning i anmeldelser om bedrageri

<https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=38285> — Fald i anmeldte bedragerier

Betænkninger

Betænkning nr. 1032, (København 1985), *Straffelovrådets betænkning om datakriminalitet*

Betænkning nr. 1417, (København 2002), *Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet*

Retspraksis

AM.2011.01.20B4

AM.2011.10.31B5

AM.2012.02.16B3

AM.2013.03.19B2

AM.2014.04.23.B

Tfk.2000.93

TfK.2004.35.Ø

TfK.2009.48.Ø

TfK.2010.494.Ø

TfK.2011.184.Ø

TfK.2011.388.Ø

TfK.2011.396/2.Ø

TfK.2011.634/2.V

TfK.2013.415.Ø

TfK.2013.1080.V

TfK.2014.577.V

TfK.2015.289.Ø

TfK.2015.443.Ø

TfK.2015.590.V

TfK.2015.653.V

TfK.2015.906.V

TfK.2016.374.V

TfK.2016.779.Ø

TfK.2016.939.V

TfK.2016.1218.V

TfK.2017.9.V

TfK.2017.124.Ø

TfK.2017.934.V

TfK.2017.1158/2.Ø

TfK.2018.751.V

TfK.2019.1071/2.Ø

TfK.2022.462.Ø

U.1989.708

U.1997.246.Ø

U.2000.1881/1.Ø

U.2001.1980/2.Ø

U.2001.1980/2.H

U.2004.2733.H

U.2004.2870.Ø

U.2005.666.H

U.2008.1063.Ø

U.2014.1241.V

U.2014.1688.V

U.2015.3399.H

U.2017.3056.V

U.2023.1476.H

Rapporter, redegørelser og årsberetninger

Anklagemyndighedens årsberetning, (1989)

Anklagemyndighedens årsberetning, (1990)

European Committee on Crime Problems, Computer-related Crime, 1990

<https://em.dk/media/14566/redegoerelse-om-danmarks-digitale-vaekst-2022.pdf> -Redegørelse om Danmarks digitale vækst 2022

<https://www.justitsministeriet.dk/wp-content/uploads/2021/08/Aftale-om-politiets-og-anklagemyndighedens-oekonomi-2021-2023.pdf>-Aftale om politiets og anklagemyndighedens økonomi 2021-2023