Aalborg Universitet – Kandidatspeciale 2023

Anvendelsen af Straffelovens § 279 a om databedrageri

I samspil med underslæb og mandatsvig, jf. Straffelovens §§ 278 & 280

Jonas Krigaum Nielsen

Studienr. 20185715

1. Titelblad

Forfatter: Jonas Krigbaum Nielsen

Studienummer: 20185715

Uddannelse: Jura

Eksamenstype: Kandidatspeciale

Uddannelsesinstitution: Aalborg Universitet

Vejleder: Birgit Feldtmann

Titel: Anvendelsen af straffelovens § 279 a om databedrageri i samspil med underslæb og mandatsvig i straffelovens §§ 278 og 280

Engelsk titel: The application of Criminal Code § 279 a on data fraud in conjunction with embezzlement and breach of trust in Criminal Code §§ 278 and 280.

Retsområde: Formueforbrydelser og cyberkriminalitet

Antal anslag: 96.046 (bevis på sidste side)

Antal sider (af 2400 tegn): 40

Afleveringsdato: 17. Maj 2023

Indhold

2. Abstract

In response to the increasing threat and growing use of technology in economic crime, Section 279 a of the Criminal Code on data fraud was introduced in 1985. Since then, data fraud has remained a serious threat to businesses, individuals, and society. As technology continues to evolve, it becomes increasingly easier for cybercriminals to commit such crimes. The recent years, partly due to covid-19, have been characterized by increased focus on data protection and personal information, making data fraud even more severe and relevant. As we move further into this unexplored and challenging landscape. We must dive further into the legislation that is designed to protect us from cybercrime. In this thesis we take a closer look at one of the most relevant paragraphs of the Danish criminal law when it comes to dealing with cybercrime. One of the central paragraphs in this context is, as mentioned, Section 279 a, which deals with data fraud. This paragraph is tailored to counter the increasing threat from frauds that, among other things, involve the manipulation of electronic data processing to achieve financial gain. Furthermore, the thesis will uncover the field of application for the provision and some of the provisions of the Criminal Code, whose field of application is close to Section 279 a's, specifically embezzlement, fraud, and breach of trust in Sections 278, 279, and 280 of the Criminal Code.

This thesis aims to examine the application of Criminal Code § 279 a on data fraud in conjunction with embezzlement and breach of trust in Criminal Code §§ 278 and 280. It can be difficult to separate their areas of application from each other and when these are combined, it can lead to even more complex and extensive cases. The thesis will be using the method of legal dogmatics to analyze and describe applicable law. The thesis will describe the field of application of Criminal code §§ 278, 279, 279 a and 280. In connection with this, §§ 279, 279 a will be compared, followed by comparative analysis of §§ 279 a, 278 and 280. Finally, there will be an analysis of case law and a conclusion where all the above-mentioned descriptions and analyses will be included. Ultimately, it will be discussed whether the Danish cybercrime legislation is too broad or even outdated.

The conclusion of this thesis tells us that, the field of application of Criminal code §§ 279 a, 278 and 280 is strongly connected. In many cases, the broad scope of the paragraphs will cause them to overlap. Furthermore, it will be seen that many cases of mandate fraud and embezzlement could be punished for data fraud. Specifically in cases where data processing has been manipulated.

3. Indledning

I begyndelsen af det 21. århundrede, da teknologiens lys strålede klart, og digitaliseringens tidsalder bredte sig over verden voksede en skjult trussel i skyggerne. Fænomenet cyberkriminalitet, som indtil nyere tid kun blev sat i sammenhæng med detektivromaner og Hollywood-film. Denne type kriminalitet har i nyere tid begyndt at tage form og udfolde sig som en uberegnelig virus. Over de seneste år er vores afhængighed af teknologi vokset eksponentielt.[1] Med denne afhængighed fulgte en stigende sårbarhed for kriminelle, som ønskede at udnytte teknologien til deres fordel. Der kunne være tale om enkelte phishing-angreb, hvor "Mathias fra banken" ringede og franarrede dig dine dankortoplysninger,[2] komplekse identitetstyverier[3], fra cybermobning til avanceret industrispionage, begyndte cyberkriminalitet at ændre form og intensitet. Som følge af den teknologiske udvikling er metoderne til at udføre forbrydelser blevet mere l, dem som udfører de kriminelle handlinger er blevet dygtigere og mere kreative[4] og ondsindede programmer, som vira og malware, er blevet sværere at bekæmpe.[5]

Som reaktion på den stigende trussel og stigende brug af teknologi i økonomisk kriminalitet blev Straffelovens § 279 a om databedrageri i 1985 introduceret. Siden da er databedrageri forblevet en alvorlig trussel mod virksomheder, privatpersoner og samfundet som helhed.[6] Som teknologien fortsætter med at udvikle sig, bliver det stadig nemmere for cyberkriminelle at udføre sådanne forbrydelser. De seneste år har, blandt andet på grund af covid-19, været præget af øget fokus på databeskyttelse og personlige oplysninger, hvilket har gjort databedrageri endnu mere alvorligt og relevant.

Mens vi bevæger os længere ind i dette uudforskede og udfordrende landskab, hvor cyberkriminalitet bliver mere indviklet og listigt står det klart, at vi må dykke dybere ind i noget af det lovgrundlag, der er designet til at beskytte os mod forbrydelser i det digitale landskab. I dette speciale tager vi et nærmere kig på én af de mest relevante bestemmelser i straffeloven, når det gælder håndtering af cyberkriminalitet. En af de centrale bestemmelser i denne sammenhæng er som sagt § 279 a, der omhandler databedrageri. Denne bestemmelse er skræddersyet til at imødegå den stadig stigende

[1] Julie Schneider, Berlingske, 08-07-2021
[2] Charlotte Hansen, TV2, 11-05-2023
[3] Digitaliseringsstyrelsen, 02-2021
[4] Camilla Bøgeholt Lund, TV2 Fyn, 23-01-2017
[5] Katie Chadd, Cybercrime Magazine, 30-11-2020
[6] Danmarks statistik, 02-02-2023

trussel fra bedragerier, som blandt andet involverer manipulation af elektroniske databehandlinger for at opnå økonomisk gevinst. Endvidere vil specialet afdække anvendelsesområdet for bestemmelsen og nogle af straffelovens bestemmelser, hvis anvendelsesområde ligger nær § 279 a's, navnlig underslæb, bedrageri og mandatsvig i straffelovens §§ 278, 279 og 280.

I dette speciale undersøges samspillet mellem straffelovens bestemmelser om databedrageri, jf. § 279 a og de tidligere nævnte bestemmelser - mandatsvig, jf. § 280 og underslæb, jf. § 278. Det kan være svært at adskille deres anvendelsesområder fra hinanden og når disse kombineres, kan det føre til endnu mere komplekse og omfattende sager.

4. Metodeafsnit

I dette speciale anvendes den retsdogmatiske metode til at analysere og beskrive gældende ret.[7] Formålet med anvendelsen af metoden er, at besvare specialets problemstilling ved at belyse og finde ny viden om:

Samspillet mellem databedrageri i strfl's § 279 a om databedrageri og strfl's §§ 278 og 280 om underslæb og mandatsvig. Herunder ligheder, forskelle og tilfælde af overlap af anvendelsesområderne.

Den retsdogmatiske metode har sit udgangspunkt i de relevante retskilder, herunder loven, retspraksis, sædvaner og forholdets natur. Disse retskilder udgør grundlaget for at beskrive og analysere den gældende ret.[8]

I projektet anvendes varierede kilder. Der vil i den indledende del af projektet blive anvendt artikler og hjemmesider, fra anerkendte danske og internationale institutioner og virksomheder, til afdækning af begrebet cyberkriminalitet og dets udvikling, herunder statistikker. Disse statistikker anvendes endvidere med respekt, for det store mørketal der måtte være i forbindelse med cyberkriminalitet.[9] Disse kilder anvendes alene i et historisk perspektiv og må ikke anses som juridisk litteratur. Blandt andet i forbindelse med begrebet cyberkriminalitet, vil der blive anvendt udvalgsbetænkninger. Disse skal anses som forarbejder og indeholder oplysninger om lovgivers hensigt med for eksempel et lovforslag. Disse vil blive anvendt til fortolkning[10]. Endvidere bliver der i store dele af specialet anvendt retslitteratur, herunder i vidt omfang kommenteret straffelov speciel del 12. udgave, af 2022. Retslitteratur, er ikke en retskilde, men bidrager til fortolkning og inspiration.[11]

Ydermere anvendes, der retskilder i form af straffeloven (herefter omtalt "strfl") og retspraksis. Retspraksis refererer til domstolenes afgørelser, som bidrager til vores forståelse af retstilstanden.[12] Ved at anvende specifikke domme vedrørende databedrageri, underslæb og mandatsvig (og flere), vil samspillet mellem disse forbrydelser undersøges. Alderen på denne retspraksis varierer, og der

[7] Munk-Hansen, Carsten, "Retsvidenskabsteori", 2022, s. 211
[8] Ibid., s. 205
[9] Astrid Søndberg mf., TV2, 07-04-2016
[10] Munk-Hansen, Carsten, "Den Juridiske Løsning", 2021, s. 54
[11] Ibid., s. 80
[12] Ibid., s.61-62

henvises til flere ældre domme i beskrivelsen af bestemmelserne i de første afsnit. Dette udgør ikke et problem, da de stadig anses for at være gældende og er blevet anvendt i nyere juridisk litteratur, herunder kommenteret straffelov speciel del 12. udgave, af 2022.

Førend vi når til specialets hovedfokus, vil specialet behandle begrebet cyberkriminalitet og kort give et indblik i den teknologiske udvikling for cyberkriminalitet, da dette beskriver, hvorfor fokusset på blandt andet databedrageri kun fortsat bliver mere relevant. Derudover vil der af kontekst og metodemæssige hensyn kort beskrives straffelovens anvendelsesområde, herunder bl.a. legalitetsprincippet, fortsæt, forsøg og medvirken. Dette bidrager i forståelsen af disse begreber, når de nævnes i forbindelse med retspraksis i den sidste del af specialet. Af samme årsag følger dernæst et afsnit om strfl's kapitel 28 (formueforbrydelser), hvorefter de relevante bestemmelser for specialet beskrives gennemgående. Denne beskrivelse indeholder også en gennemgang af strfl's § 279 om bedrageri, da dette er nødvendigt for at kunne forstå den fulde kontekst af § 279a. Efter gennemgangen af de relevante bestemmelser anvendes retspraksis til at analysere forholdet mellem § 279 a og §§ 278, samt 280. Afslutningsvis vil specialet diskuterer, hvorvidt den danske lovgivning er for bred og måske forældet på området for cyberkriminalitet. Dette sker ved en kort komparativ analyse er enkelte bestemmelser i den danske straffelov og den tyske "strafgesetzbuch".

4.1 Afgræsning

I dette speciale vil der være fokus en række bestemmelser i straffelovens kapitel 28 om formueforbrydelser, som har relevans i forhold til databedrageri, hvorfor der afgrænses fra andre typer cyberkriminalitet, eksempelvis hacking, jf. strfl's § 263 stk. 2. Der skal i forbindelse med redegørelse og analyse af relevante bestemmelser afgrænses fra strfl's §§ 276-277, 281-283 og 297-305. Nogle af disse vil dog kort blive nævnt. Specialet vil endvidere ikke vedrøre straffelovens almindelige del. Der vil dog kort blive behandlet "*forsæt*" i forbindelse med beskrivelsen af formueforsæt i afsnittet om formueforbrydelser. Specialet vil kun have fokus på den danske strafferet, afgrænses derfor fra eventuel international lovgivning og retspraksis, samt eventuel anden dansk lovgivning til har til sinde at beskytte dataens integritet. Der vil til slut i diskussionen, være fokus på datakriminalitet, hvorfor underslæb og mandatsvig ikke vil blive behandlet.

5. Cyberkriminalitet

Begrebet cyberkriminalitet eller IT-kriminalitet har ikke en fast definition, da det af flere omgange er blevet beskrevet på forskellige måder. Dog har Straffelovrådet i betænkning nr. 1032/1985, beskrevet "datakriminalitet i egentlig forstand", som de forbrydelser, "*der rummer en anvendelse af den for databehandling særegne teknik med hensyn til registrering, opbevaring, bearbejdelse og brug af oplysninger"*. Her nævnes også begrebet *"datakriminalitet i vid forstand",* som er forbrydelser, *"der ligger før eller efter databehandlingen",* eller forbrydelser der implicerer *"tyveri af udstyr eller fysisk hærværk mod det".* Dertil kan det nævnes, at rådet har i deres betænkning beskæftiget sig med forbrydelser,[13] "hvor IT indgår som mål eller middel eller forudsætning for handlingen".[14]

Det Kriminalpræventive Råd (herefter DKR) definerer cyberkriminaliteten som en *"paraplybetegnelse for en lang række kriminelle aktiviteter, hvis fællesnævner er, at computerbaseret teknologi"*[15] og skelner her mellem 3 forskellige kategorier af cyberkriminalitet. Først nævnes "Computer-Integritetsforbrydelser", som har til mål at skade en persons eller en virksomheds it-system. Herunder nævnes blandt andet hacking, forskellige typer vira og DDoS-angreb. Dernæst nævnes "Computer-assisterede forbrydelser". Rådet taler i dette tilfælde om bedrageri foretaget ved hjælp af IT. Altså den for specialet nærværende forbrydelse; databedrageri. Herunder findes blandt andet phishing og netbanksvindel. Til sidst nævner DKR kategorien "Computer-indholdsforbrydelser". Disse forbrydelser vedrører besiddelse eller distribution af kriminelt materiale. Dette omfatter blandt andet deling eller besiddelse af børnepornografi, racistisk indhold og voldelige billeder eller videoer.[16]

Hvis man skal give en kort og forståelig beskrivelse af begrebet, kan det ud fra ovenstående siges, at cyberkriminalitet eller IT-kriminalitet refererer til forbrydelser, der involverer anvendelse af computere (herunder smartphones, tablets m.v.), internettet eller anden digital teknologi. Begrebet omfatter forskellige som tidligere nævnt en lang række forbrydelser, som i deres helhed er blevet en

[13] Betænkning nr. 1417, s. 22
[14] Ibid.
[15] DKR, 2018, "Cybercrime - Når kriminaliteten rykker online",
[16] DKR, 16-11-2022, "IT-kriminalitet i tal"

stor trussel mod privatpersoner, men også virksomheder og offentlige myndigheder.[17][18][19] Udviklingen af dette vil blive behandlet i kommende afsnit.

5.1 Den teknologiske udvikling

Det er svært at præcist at sige, hvor langt tilbage cyberkriminalitet kan spores, da der er delte meninger herom blandt eksperter. Nogle mener, at det kan spores helt tilbage til 1834, hvor to personer stjal data og fik adgang til finansielle markeder, ved at infiltrere det franske telegrafsystem.[20] Andre mener, at de første former for rigtig cyberkriminalitet vandt frem i 1950'erne, i form af "*Phone-Phreaking*"[21], der gik ud på at "stjæle" telefonopkald, så man kunne ringe gratis[22]. Det menes, at denne form for "telefonhacking" var, hvad der blev startskuddet til, det vi i dag kender som hacking, som først i midten af 1960'erne begyndte at vinde frem. Dog var målet med hacking ikke ondsindet eller med vinding for øje, men blev blot udført af det fåtal af personer, der havde adgang til den nye teknologi. Herunder typisk nysgerrige studerende eller forskere på universiteter, der ønskede at forbedre systemerne.[23]

Hacking blev dog ikke ved med, kun at forbundet med godsindede handlinger. I 1986 trådte cyberkriminalitet for alvor i karakter, da en tysker hackede sig ind i internettets forgænger "*ARPANET*", og gennem dette fik adgang til det amerikanske forsvarsministerium Pentagon og adskillige andre militære computere, hvorefter han havde til hensigt at sælge informationer til den sovjetiske efterretningstjeneste KGB[24][25]. Året efter, 1987, blev Vienna og Cascade Virusset udviklet, dette var de første eksempler på et program, der infiltrerede computersystemer, og menes at være, hvad vi i kender som, malwarerens forgænger. I takt med udviklingen blev hackerne mere sofistikerede og dermed også deres mål. Allerede i 80-90'erne blev målet for hackerne at infiltrere virksomheder, for at stjæle følsomme oplysninger eller beskadige deres systemer.[26]

[17] Center for cybersikkerhed, "Cybertruslen"
[18] Julie Schneider, Berlingske, 08-07-2021
[19] Europa-Parlamentet, 23-11-2022, "Hvorfor er cybersikkerhed vigtigt, og hvad koster cyberangreb EU?",
[20] BlueVoyant, 2022," Cybercrime: History, Global Impact & Protective Measures"
[21] Katie Chadd, Cybercrime Magazine, 30-11-2020
[22] Wikipedia, 2019," Phone-Phreaking"
[23] Katie Chadd, Cybercrime Magazine, 30-11-2020
[24] Wikipedia, 2023, "KGB"
[25] Katie Chadd, Cybercrime Magazine, 30-11-2020
[26] Ibid.

Som følge af internettets fødsel og denne stigende trussel begyndte regeringer og virksomheder i 1990'erne at tage cybersikkerhed mere alvorligt. Her startede oprettelsen af cybersikkerheds-afdelinger og udviklingen af antivirusprogrammer til at beskytte mod cybertrusler for alvor. Mod slutningen af 1990'erne var e-mail blevet udbredt, og selvom det lovede at revolutionere kommunikation, åbnede det også op for en ny indgang for vira og andre ondsindede handlinger.[27]

Siden århundredeskiftet har den teknologiske udvikling taget til, og cyberkriminalitet vundet yderligere terræn. Dette førte blandt andet til kontroversielle og meget omtalte sager om cyberkriminalitet. Herunder blandt andet i 2013; Edward Snowden, som kopierede klassificerede informationer fra den amerikanske sikkerhedstjeneste NSA og delte dette med verden eller i 2019; hvor den New Zealandske børs blev ramt af adskillige DDoS-angreb. Den skræmmende udvikling satte i den grad sine spor i cyberkriminalitetens omkostninger, hvor estimater fra Europa Kommissionen har vist, at omkostningerne blev fordoblet i årrækken 2015-2020, hvor man i 2020 estimerede de samlede omkostninger i verden til at være 5,5 billioner euro, svarende til ca. 41 billioner danske kroner.[28]

I 2019 kom en ny faktor i spil på det cyberkriminelle område; hjemmearbejde som følge af Covid-19. Dette resulterede i at virksomheder og myndigheder skulle sætte yderligere fokus på en ny forværret cybertrussel. Her var blandt andet tale om Covid-19 tematiserede forbrydelser, som eksempelvis phishing mails. Center for cybersikkerhed udtalte i april 2020, at trusselsbilledet ikke var ændret, men at der var forøget risiko for at cyberkriminelle ville lykkes med deres angreb. Dette skyldtes blandt andet at folk var ude af deres sædvanlige "*arbejdsrammer*", når de arbejdede hjemmefra.[29] Som modsvar på denne trussel vedtog regeringen d. 2. april 2020, en forøget strafferamme for lovovertrædelse som havde baggrund i eller sammenhæng med covid-19. Denne strafferamme bev indført i straffeloven som § 81 d, og omfattede "*hjælpepakkesvig*"[30], men også andre lovovertrædelser med baggrund i covid-19, jf. § 81 d, stk. 4. Ved brug af denne bestemmelse blev det således en skærpende omstændighed for alle lovovertrædelse, bl.a. databedrageri, hacking m.v., hvis disse var sket med baggrund i covid-19. Bestemmelsen er dog i dag afskaffet.

[27] Ibid.
[28] Europa-Parlamentet, 23-11-2022, "A cybersecure digital transformation in a complex threat environment"
[29] Center for cybersikkerhed, 03-04-2020, " Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien"
[30] Kromann Reumert, 06-04-2020

Selvom cyberkriminalitet har været i fremdrift i en længere årrække, viser det dog, at tekniske tiltag fra myndigheder og banker i samspil af danskernes stigende opmærksomhed har fået anmeldelser af IT-forbrydelser til at falde. Dette kan ses på tal fra DKR, der viser et fald fra 194 tusinde ofre for cyberkriminalitet i 2020 til 150 tusinde ofre i 2021. I denne forbindelse nævner DKR også, at særligt misbrug af betalingskort er faldende.[31] Dette udsagn kan også støttes i tal fra Finans Danmark, der viser, at banker i 2022, fik stoppet netbanksvindel for over 113 millioner kroner. Dog viser samme tal at de cyberkriminelle i 2022, bare i Danmark slap væk med 96 millioner kroner ved at franarre folk personoplysninger og derved få adgang til folks netbank.[32] Selvom man i 2020-21 kan se et fald af anmeldte IT-forbrydelser, betyder det ikke nødvendigvis at problemet er forbipasserende. Det kan endda blot være et billede af, at de cyberkriminelle er begyndt at tænke større og den enkelte forbrydelse, måske blot er blevet mere omfattende og omkostningsfuld for dens ofre[33]. EU-kommissionen spår nemlig, at cyberkriminalitet kun vil blive endnu mere omkostningsfuld frem mod 2025, hvor man estimerer, at omkostningerne for cyberkriminalitet samlet vil stige med 25 milliarder euro, svarende til ca. 186 milliarder danske kroner.[34]

6. Formueforbrydelser (Straffelovens kapitel 28)

Strfl's kapitel 28 omhandler formueforbrydelser og fastsætter strafansvar for forskellige former for økonomisk kriminalitet. Kapitlet beskriver forskellige formueforbrydelser[35], blandt andet de nærværende bestemmelser for dette speciale, der som tidligere nævnt er databedrageri, mandatsvig og underslæb, jf. strfl's §§ 279 a, 280 og 278. Kapitlets bestemmelser kan inddeles i to grupper. Først *"berigelsesforbrydelser"* §§ 276-284 og 288[36], hvor økonomisk vinding er en del af gerningsindholdet og hvor der i denne forbindelse "*subjektivt*" også skal være forsæt til økonomisk vinding fra gerningspersonens side, altså "*berigelsesforsæt*". Denne økonomiske vinding kan dog, tilfalde andre end gerningspersonen selv – "*tredjemand*". Generelt fortælle om forsæt kan siges, at *"man har forsæt til at gøre noget, hvis man gør det 'med vilje'"*, men man burde indse, at sine *"handlinger med overvejende sandsynlighed vil medføre det pågældende retsbrud*".[37] I disse tilfælde vil

[31] DKR, Via Ritzau, 21-04-2022
[32] Freja Thorbech, Finansforbundet, 08-05-2023,
[33] Andrew Douthwaite, Virtualarmour, 26-10-2022
[34] Europa-Parlamentet, 23-11-2022, "A cybersecure digital transformation in a complex threat environment"
[35] Baumbach, Trine mf. "Udvalgte delikter i straffeloven – en indtroduktion", 2021, s. 81
[36] Herunder også 285-287 - Dette er dog kun udmålingsbestemmelser.
[37] E-lov, juridisk ordbog, 05-10-2014, "forsæt",

berigelsesforsæt simplificeret være tilfælde, hvor foretager en handling med økonomisk vinding til sig selv eller andre for øje, hvor man vidste eller burde indse, at handlingen var lovstridig. Derudover gælder det med få undtagelser for de resterende formueforbrydelser i kapitel 28, at der som udgangspunkt ikke er et krav, om hvorvidt, der skal foreligge forsæt til økonomisk vinding, men blot at der er lidt et økonomisk tab/formuetab[38]. Dertil bør det også nævnes, at kravet for et formuetab, ved for eksempel bedrageri, normalvis ikke er opfyldt, hvis offeret alligevel opnår en ydelse, der har samme værdi som den de giver til gengæld, jf. JD 1940.130 U, hvor tiltalte havde serveret whisky i flasker fra et andet whiskyfabrikat. Her blev det ikke godtgjort, at den påfyldte whisky var billigere end den oprindelige, hvorfor der ikke var sket formuetab. Dog er dette blevet delvist ændret i U 1980.628 V, hvor der godt kan straffes, for i dette tilfælde bedrageri, uden at der reelt er sket et formuetab, hvis der systematisk udvises *"overfor personer, der på grund af ukyndighed mv. er særlig lette ofre".*[39] For de bestemmelser der behandles nedenfor (her bedrageri, databedrageri, underslæb og mandatsvig, jf. strfl's §§ 279, 279 a, 278 og 280) er det ligeledes gældende, at vedkommende der har udført den kriminelle handling har indset, at vedkommendes "adfærd medførte en vis risiko for tab", jf. blandt andet, TfK 2008.647 Ø, hvor tiltalte (for i dette tilfælde bedrageri) havde underskrevet lånedokumenter i hans kones navn uden hendes medvirken. Her lød ifølge tiltalen; *"Lån- og kreditgiverne blev ved nedenstående handlinger bragt i en vildfarelse om, at tiltalte og H i forening indgik aftaler om lån og kredit og led herved - eller var i væsentlig risiko for at lide - tab svarende til de nævnte beløb.*

Til sidst bør ved gennemgang af kapitel 28 nævnes, at der tilsvarende er inkorporeret udmålingsbestemmelser i kapitel 28, herunder blandt andet §§ 285-287. I forbindelse med klarlægningen af kommende bestemmelsers, strfl's §§ 279, 279 a, 278 og 280, er der endvidere fastsat fælles strafferamme og straffes *"med fængsel indtil 1 år og 6 måneder*", jf. strfl's § 285, stk. 1 eller med *"fængsel indtil 8 år"* i tilfælde af forbrydelse af særlig grov beskaffenhed, jf. strfl's § 286, stk. 2, i forbindelse med vurderingen heraf indgår "*udførselsmetoden*", hvorvidt der er tale om organiseret kriminalitet, jf. ordlyden *" fordi forbrydelsen er udført af flere i forening"* og omfanget af den vinding der er opnået eller tilsigtet. Kommenteret straffelov siger herom, at afgræsningen mellem de forskellige forbrydelser på denne måde egentlig mister sin praktiske betydning.[40] Til sidst er det vigtigt

[38] Baumbach, Trine mf. "Udvalgte delikter i straffeloven – en indtroduktion", 2021,
[39] Elholm, Thomas mf. "Kommenteret straffelov – Speciel del", 2022, s. 687
[40] Ibid., s. 652

at nævne, at gerningsindholdet i en del formueforbrydelser overlapper hinanden.[41] Dette vil også komme til udtryk i forbindelse med besvarelsen af specialets problemformulering.

7. Databedrageri

7.1 Bedrageri, jf. straffelovens § 279

I dette afsnit vil strfl's § 279 behandles. Dette er nødvendigt for at forstå sammenhængen og forskellen på bedrageri og specialets hovedbestemmelse, nemlig strfl's § 279 a. Denne bestemmelse omhandler bedrageri og indeholder bestemmelser om, hvordan denne forbrydelse straffes i Danmark. Ordlyden er som følger:

> ***"§ 279.*** *For bedrageri straffes den, som, for derigennem at 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."*

Bedrageri defineres i straffeloven som en forbrydelse, hvor en person på en vildledende måde får en anden person til at handle eller undlade at handle til skade for denne person eller en tredjepart. For at forstå bestemmelsen til fulde bør der redegøres for to elementer som bestemmelsen indeholder; påvirkning af en handling ved vildfarelse og de økonomiske konsekvenser, herunder tab eller risiko for tab og vinding.[42] I forhold til de økonomiske konsekvenser, skal det her nævnes, at bedrageri er en berigelsesforbrydelse, hvorfor der er krav om berigelsesforsæt.

En "*vildfarelse*" defineres i litteraturen som *"en urigtig antagelse om et forhold, som indgår i den pågældendes motivationsgrundlag"*[43] og derfor kræver, at gerningspersonen får modparten til at udføre en handling ved at få dem til at tage fejl af en situation, eller tro på noget der ikke er sandt.[44] Et eksempel på dette kan være et bilsalg, hvor sælger giver køber urigtige informationer om bilen, som er afgørende for at køber vil købe bilen, jf. for eksempel U 1992.65/1 Ø, hvor sælger troede, at der var et ejendomsforbehold på en bil og underskrev erklæring om, at der ikke var ved videresalg af

[41] Baumbach, Trine mf. "Udvalgte delikter i straffeloven – en indtroduktion", 2021, 82
[42] Elholm, Thomas mf. "Kommenteret straffelov – Speciel del", 2022, s. 148
[43] Ibid.
[44] Ibid., s. 683

denne.[45] I dette tilfælde var der dog ingen reel vildfarelse, da ejendomsforbeholdet var ugyldigt og sælger blev derfor kun straffet for forsøg på bedrageri, jf. strfl's § 279, jf. § 21. Denne dom viser dog også, at du godt kan straffes selvom en vildfarelse reelt ikke indtræder, men at det blot er nok at du har haft forsæt til, at foretage vildfarelsen. For at der er tale om en vildfarelse er en ydermere en betingelse, at der skal indgå menneskelig forestilling. Det vil sige at alt, der omfatter manipulation af IT-systemer eller anden teknologi, ikke kan være bedrageri i sig selv, men derimod vil være omfattet af for eksempel databedrageri i strfl's § 279 a.[46] Denne bestemmelse vil blive behandlet i kommende afsnit. Vildfarelsen skal ydermere fremkaldes, bestyrkes eller udnyttes af gerningspersonen. Dette kan eksempelvis ske ved at "pynte" på sandheden som eksempelvis i førnævnte dom, U.1992.65/1 Ø, ved at underskrive erklæring om intet ejendomsforbehold, selvom de troede, at der egentlig var et. Hvorvidt fortielser bliver omfattet, er et spørgsmål om, hvorvidt en bestemt oplysning er relevant, for at den vildledte vil foretage handlingen.[47]
Hertil kan det nævnes, at der i U 1956.131 V, hvor der blev solgt varebil, hvor sælger havde kendskab til og repareret midlertidigt repareret en motorblok uden at oplyse herom, ikke var tale om en fortielse, da sælger havde sagt til køber, at bilen var købt som beset, og at der ingen garanti var mod sprængninger i motorblokken. I dette tilfælde udtalte byretten at sælgerens udsagn måtte udløse en form for undersøgelsespligt hos køber. Dog ville det modsætningsvist nok have været en fortielse, hvis ikke sælger havde udtalt at der ingen garanti var mod sprængninger i motorblokken.
Fuldbyrdelsesmomentet for bedrageri, er når der indtræder et formuetab eller i nogle tilfælde, når der indtræder en væsentlig risiko for formuetab.

7.2 Databedrageri, jf. straffelovens § 279 a

I dette afsnit behandles strfl's § 279 a om databedrageri. Dette er nødvendigt i besvarelsen af problemformuleringen, da forståelsen af bestemmelsen danner ramme for at afdække samspillet mellem bestemmelsen og henholdsvis mandatsvig og underslæb.

Bestemmelsen er indført i 1985, som reaktion på den stigende teknologiske udvikling, og supplement til bedrageribestemmelsen i strfl's § 279[48]. Bestemmelsen omhandler databedrageri og angår

[45] Ibid., s.149
[46] Ibid., s. 683
[47] Ibid., s. 684
[48] Betænkning nr. 1032

retsstridige ændringer, tilføjelse eller sletninger af oplysninger eller programmer i elektronisk databehandling eller andre måder, hvorpå der forsøges at påvirke resultatet af sådan databehandling med økonomisk vinding for øje.

Ordlyden af bestemmelsen om databedrageri er som følger:

*"**§ 279 a.** 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."*

Som nævnt i afsnit 6.3 er databedrageri berigelsesforbrydelse, hvorfor der er krav om berigelsesforsæt. Dette fremgår også af bestemmelsens ordlyd i form af "*at skaffe sig eller andre uberettiget vinding"*. Det kræver således, at gerningspersonen har forsæt til økonomisk vinding og derigennem ligeledes forsæt til tab eller væsentlig risiko for tab hos modparten. Strfl's § 279 a har endvidere et fremrykket et fremrykket fuldbyrdelsesmoment. Tidspunktet for fuldbyrdelse indtræder allerede ved handlingen i 1. led, altså på det tidspunkt, hvor der retsstridigt ændres, tilføjes eller slettes oplysninger eller programmer. Det forventes her, at personen som udfører denne handling ikke skal gøre mere for at opnå den økonomiske vinding.[49]

Derudover kræver databedrageri ifølge ordlyden, at der indgår "*elektroniks databehandling*". Dette kræver, at der et "*anlæg*", hvor der skal ændres, tilføjes eller slettes oplysninger eller programmer fra. Der findes ikke en specifik definition på dette "*anlæg*", men ifølge litteraturen bør definitionen af dette *"udlægges i dagligsproget"*.[50] Dette kunne eksempelvis være en computer eller anden teknologi, herunder også smartphones m.v.

For at fastlægge anvendelsesområdet for strfl's § 279 a er det nødvendigt først, at klarlægge hvad bestemmelsens ordlyd i henholdsvis 1. og 2. led rummer. I 1. led beskrives den kriminelle handling, som: *"at ændre, tilføje eller slette oplysninger eller programmer"*.[51] Det kunne for eksempel være en situation, hvor en person foretager ændringer, eller tilføjer betalingsoplysninger i en netbank, som de har fået adgang til, for uberettiget, at overfører penge til sig selv. Dette kan blandt andet ses

[49] Elholm, Thomas mf. "Kommenteret straffelov – Speciel del", 2022, s. 694
[50] Ibid., s. 693
[51] Ibid.

i TfK 2010.785 V, hvor bogholder overfører penge fra sin arbejdsgivers konto til sin egen, ved brug af netbank. For så vidt angår *"sletning*" behøver der ikke være tale om en fuldkommen sletning eller hindring, men også en delvis sletning eller hindring vil være nok til, at handlingen vil være omfattet af bestemmelsen.[52] Endvidere fungerer 2. led som en udvidelses eller et opsamlingsled, for det som ikke falder under bestemmelsens 1. led. Kommenteret straffelov specielle del nævner blandt andet at det kan være situationer, hvor "*udenforstående gerningspersoner udnytter godtroende ansatte ved anlægget".* Et eksempel på dette kunne være et phishing-angreb. I dette tilfælde kan gerningsmanden sende en mail der for den uvidende ser harmløs ud til en person i en virksomhed. I sådanne mails udgiver gerningspersoner ofte sig for at være arbejdskoleger eller folk, der må den ene eller anden måde kan komme til dig gode rent økonomisk. Hvis vedkommende som har modtaget e-mailen, stoler på den og følger de instrukser, der er angivet deri, kan de give gerningspersonen i nogle tilfælde give adgang til persondata, virksomhedsdata m.v. Dette kan således gøre at gerningspersonen får adgang til at ændre, tilføje eller slette oplysninger eller programmer som beskrevet i strfl's § 279 a. Sådan en situation vil være en overtrædelse af databedragsbestemmelsen, fordi gerningsmanden opnår adgang ved at udnytte den godtroende ansat. Dette ville udgøre en overtrædelse af § 279 a, fordi gerningsmanden, selvom de ikke er en medarbejder eller på anden måde formelt associeret med anlægget, opnår adgang til og manipulerer data gennem udnyttelse af en godtroende medarbejder.

I forbindelse med klarlægningen både strfl's § 279 og særligt § 279 a, er det vigtigt at omtale brugen af betalingskort, mere specifikt dankort, i forbindelse hermed. Her nævnes det blandt andet i litteraturen, at misbrug af eget dankort, der er skyld i et overtræk, kan straffes efter strfl's § 279 om bedrageri, hvis beløbet der trækkes over, overstiger nets' betalingsgaranti. Her vil der som udgangspunkt være tale om bedrageri overfor butikken, man har handlet i, hvis den er fysik. Modsat vil der derimod være tale om databedrageri, jf. § 279 a, hvis der er handlet på nettet. Udover sondringen mellem databedrageri og bedrageri vil sådanne tilfælde også henføres under mandatsvig, jf. strfl's § 280, stk. 1, nr.1, for så vidt angår den del af overtrækket som er dækket af nets' betalingsgaranti. Der i forbindelse med anvendelse af dankort forskel på, hvorvidt man har vildledt en fysisk person eller om handlen blot er blevet godkendt af et IT-system.[53] Et eksempel på dette kan ses i TfK 2017.9 V, hvor frisørlærling uretmæssigt havde fået fat i oplysningerne fra arbejdsgiverens betalingskort, hvorefter hun anvendte dette til handel på nettet. Frisørlærlingen blev i landsretten dømt

[52] Ibid.
[53] Ibid., s. 688

for databedrageri, jf. § 279 a. Nærliggende den uberettigede brug af betalingskort ligger brugen af andres betalingskort gennem wallet eller andre elektroniske betalingsløsninger. Disse tilfælde vil utvivlsomt også falde under § 279 a's anvendelsesområde, jf. TfK 2022.173 Ø, hvor tiltalte havde anvendt modpartens betalingskort via en mobilbetaling-app på tankstation og TfK 2022.203 V, hvor tiltalte havde overført penge til sig selv via mobilepay. Endvidere fremgår det af litteraturen, at der ved automatiserede processer altid, vil være tale om databedrageri (herunder også ubemandede pengeautomater, tankstationer m.v. – se blandt andre TfK 2022.173 Ø ovenfor og U 2014.1688 V nedenfor). Endvidere er der stadig tale om en automatiseret proces selvom, man ved internethandel har folk i fysisk berøring med en varer i forbindelse med afsending. For at handel på nettet vil blive omfattet af bedrageribestemmelsen vil det kræve, at der er en fysisk person, der bliver vildledt i forbindelse med, at de konkret forholder sig til bestillingen og betalingen. Dertil kan også nævnes, at forhold, hvor internettet anvendes som kommunikationskanal, som udgangspunkt vil være bedrageri, jf. § 279. Dette kan blandt andet ses i TfK 2020.459 V, hvor tiltalte blev fundet skyldig i bedrageri efter at have foregivet at ville sælge golfbolde på Facebook, modtaget betaling herfor for derefter ikke at sende dem.[54]

En særdeles vigtig dom for at forstå anvendelsesområdet for bestemmelsen om databedrageri, når det omfatter svindel med hævekort, er U 2014.1688 V. Denne dom er vigtig for grænsedragningen mellem databedrageri og tyveri strfl's § 276. I denne sag blev 4 personer, dømt for databedrageri af grov beskaffenhed, jf. strfl's § 279 a, jf. § 286, stk. 2. Personerne havde anvendt stjålne dankort til at hæve store beløber på dankortterminaler, som enten var stjålne eller leveret ved at oprette virksomheder, som indgik aftaler med Nets. Dommen angik spørgsmålet om, hvorvidt "*Uberettiget brug af et dankort og en terminal til hævning"* skulle anses som databedrageri, jf. strfl's § 279 a eller tyveri, jf. strfl's § 276. Vestre landsret udtalte i dette tilfælde, at der ved en sådan transaktion sker "påvirkning af resultatet af elektronisk databehandling og dermed indgreb i grundlaget herfor". Landsretten udtaler i dommen også, at det ikke er relevant, hvorvidt en transaktion er online eller offline. Ud fra denne dom må det kunne man som udgangspunkt fastlægge at sager, hvor der er tale om "tyveri" af hævekort for efter at bruge dem til at hæve penge fra i en automat, er og vil blive set som databedrageri. Tillige kan det nævnes, at der for databedrageri ikke er krav om, at noget skal ske online, men blot at der er tale om en transaktion som påvirker resultatet af en

[54] Ibid., s. 695

databehandling. Denne dom er et klart eksempel på praksisændring hos den danske domstol, og kan ses i forhold til dommene TfK 2009.48 Ø og TfK 2021.1115 Ø.

I TfK 2009.48 Ø, som ligger før praksisændringen bliver T, dømt for tyveri, jf. strfl's § 276, for at have afluret pinkoder, stjæle hævekort og herefter at anvende dem til at hæve omkring 250 tusinde kroner, samt forsøg at hæve 20 tusinde kroner. I denne dom blev der endvidere også stjålet kontanter fra ofrenes tegnebøger. Denne dom viser, at man før U 2014.1688 V dømte for tyveri, når der blev anvendt stjålne hævekort. Lidt anderledes er dette dog i TfK 2021.1115 Ø, der på mange måder ligner de andre domme. Her havde en person også stjålet flere hævekort, samt tegnebøger med kontanter og andre genstande, for efterfølgende at hæve på kortene. Her udtalte byretten, at de ikke fandt, at praksis for denne type kriminalitet var ændret i TfK 2014.1688 V, og henførte derfor alle sagens forhold under strfl's § 276 om tyveri. Denne sag blev dog anket til landsretten, hvor der igen blev fastsat at denne type kriminalitet skal henføres til strfl's § 279 a. Gerningspersonen blev i landsretten dømt for både, databedrageri, jf. strfl's § 279 a for så vidt angår de uberettigede hævninger og henviste her til blandt andet TfK 2014.1688 V.

7.3 Sammenligning

Databedrageri og bedrageri er i sig selv begge bedrageribestemmelser, men der er uomtvisteligt en væsentlig forskel på de to bestemmelser. Ud fra ovenstående kan det konkluderes, at bedrageri og databedrageri, jf. strfl's §§ 279 og 279 a adskiller sig fra hinanden på forskellige måder. Først står det klart, at anvendelsesområdet og handlingens karakter utvivlsomt adskiller bestemmelserne. Bedrageri kan omfatte forskellige handlinger, der involverer en vildfarelse, som bestemmer modparten til en handling eller undladelse. Databedrageri specifikt fokuserer på retsstridige handlinger, der påvirker elektronisk databehandling, herunder ændringer af oplysninger eller programmer. Det skal dog nævnes, at de to bestemmelser nemt kan forveksles i sager, hvor der indgår teknologi, men hvor der også er mennesker, der muligvis kan blive vildledt. Dette kan ses i forbindelse med internethandel, hvor grænsedragningen må falde på, hvorvidt "mennesket" konkret forholder sig til bestillingen og betalingen, jf. ovenstående afsnit. Nærliggende dette er den tredje forskel, nemlig fuldbyrdelsestidspunktet. Modsat bedrageri er der i forbindelse med databedrageri i § 279 a's tilfælde et fremrykket fuldbyrdelsesmoment, hvilket gør det umuligt at anvende bestemmelsen uden, der er sket formuetab.

8. Underslæb, jf. Straffelovens § 278

I dette afsnit behandles strfl's § 278 om underslæb. Dette er nødvendigt i besvarelsen af problemformuleringen, da forståelsen af bestemmelsen danner ramme for at afdække samspillet mellem bestemmelsen og henholdsvis databedrageri og mandatsvig.

Underslæb er en berigelsesforbrydelse, der er defineret i strfl's § 278. Denne bestemmelse omhandler situationer, hvor en person uberettiget tilegner sig andres formue eller aktiver, som vedkommende har fået betroet adgang til, jf. bestemmelsens ordlyd. Underslæb i strfl's § 278 er en berigelsesforbrydelse, hvorfor der er krav om berigelsesforsæt. Dette fremgår også af § 278, stk. 1, som lyder: *"§ 278. For underslæb straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding"*. Det kræver således, ligesom ved de førnævnte bestemmelser, at gerningspersonen har forsæt til økonomisk vinding og derigennem ligeledes forsæt til tab eller risiko for tab hos modparten. Det er ligesom ved bedrageri, at der er tale om væsentlig risiko for tab. [55]

Bestemmelsen er endvidere opdelt i 3 typer, hvor den første fremgår af bestemmelsens nr. 1, og omhandler situationer, hvor gerningspersonen *"tilegner sig en fremmed rørlig ting, der er i hans varetægt, uden at forholdet falder ind under § 277".* Dette kan også kaldes "tingsunderslæb".[56] Her er det et krav, at der er tale om tilegnelse af en fremmed rørlig ting, og ligeledes, at denne ting har en økonomisk værdi.[57] Forbrydelsen fuldbyrdes endvidere ved tilegnelsen.[58] Hvad er omfattes af denne betegnelse bliver typisk behandlet ved tilfælde af tyveri efter strfl's § 276.

"*Ting*" defineres i forbindelse med tyveri, som fysiske genstande – løsøre, men også genstande, som ikke betragtes som løsøre, som bygningsdele og beplantning, jf. U 1937.376 V, hvor en person havde taget sten og sand fra en offentlig strand og U.1940.1113 Ø, hvor en person havde fældet birketræer og derved tilegnet sig disse. Desuden sidestilles "energimængder" og dyr med rørlige ting, jf. strfl's § 276, stk. 2 og U 2014.2941 V, hvor hunde blev fjernet fra kennel.[59] Endvidere defineres "*fremmed*" i litteraturen, som noget, der *"helt eller delvist tilhører en anden end gerningspersonen".* Dette udelukker, derfor underslæb, hvis tingen er ejerløs, jf. U 1942.419 Ø, hvor der blev opsamlet afskudte projektiler på en skydebane, eller tilfælde, hvor tingen alene er ejet af

[55] Ibid., s. 681
[56] Ibid., s. 673
[57] Ibid., s. 672
[58] Ibid., s. 676
[59] Ibid., s. 656

gerningspersonen.[60] Desuden bliver ægtefælles særeje, samt købte ting som endnu ikke er overgivet, anset som "*fremmed*". [61] Som tidligere nævnt er det for den fremmed rørlige ting også et krav, at det tilegnede har økonomisk værdi, jf. blandt andre U 1978.572 V, hvor tilegnede pasblanketter fra politikontor ikke havde økonomisk værdi, hvorfor tiltalte blev frifundet.

For nr. 1, er den strafbare handling tilegnelsen. Herunder gælder det, at genstanden der tilegnes af gerningspersonen, skal have befundet sig i deres varetægt. Vigtigt er her også at afgrænse fra strfl's § 277 om ulovlig omgang med hittegods[62], hvor der er tale om tilegnelse af fremmed rørlige ting, *"som ikke er i nogens varetægt, eller som ved ejerens forglemmelse eller på lignende tilfældig måde er i gerningsmandens varetægt"*[63]. Kravet for, hvorvidt der er sket tilegnelse, er som udgangspunkt at gerningspersonen betragter og behandler genstanden som var det sin egen. Til dette skal det nævnes, at der for anvendelse af nr. 1 er et krav om forsæt til tilegnelsen, hvilket gør at situationer, hvor der kun er forsæt til midlertidig anvendelse ikke vil blive omfattet af strfl's 278, stk. 1, nr. 1, men derimod strfl's §§ 293 eller 293 a (brugstyveri).

Som eksempler på forhold, der falder under tingsunderslæb i strfl's § 278, stk. 1, nr. 1, kan eksempelvis nævnes, tilegnelse eller videresalg at genstande som er lånt, leaset eller lejet, jf. U 2000.1893 Ø, hvor gerningspersonen solgte en lejet trailer og diverse værktøj som han havde lejet, U 1975.434 V, hvor gerningspersonen tilegnede sig radio som var modtaget på prøve, og TfK 2014.1035 V, hvor gerningspersonen havde leaset en bil, hvorefter han omregistrerede den til sig selv og eksporterede den til Tyskland. Ydermere må genstande, der bliver tilegnet efter, at de er overgivet til opbevaring, transport, reparation eller kommission være omfattet af nr. 1[64]. Herunder falder også situationer, hvor man foretager svigagtigt dobbeltsalg. Dette vil konkret sige, at man sælger noget, som reelt allerede er solgt til en anden køber, og på den måde modtager dobbelt betaling.[65]

Ved gennemgang af nr. 1 er det væsentligt at runde, strfl's § 278, stk. 2, der lyder således: *"Bestemmelsen i stk. 1, nr. 1, omfatter ikke dispositioner over købte genstande, med hensyn til hvilke en sælger har forbeholdt sig ejendomsret, indtil købesummen er betalt."*. Her er nævnes det, at "kreditkonsignationsforhold" ikke omfattes af tingsunderslæb. Dette kan eksempelvis være tilfælde, hvor

[60] Ibid., s. 656-657d
[61] Ibid., s. 657-658
[62] Ibid., s. 673
[63] Straffelovens § 277
[64] Elholm, Thomas mf. "Kommenteret straffelov – Speciel del", 2022, s. 673-675
[65] Ibid., s. 676

der er indgået flexleasing aftaler, hvor det er meningen, at ejendomsretten skal overgå til, leaser ved slutningen af leasingperioden.[66]

En anden type underslæb fremgår af strfl's § 278, stk. 1, nr. 2, som lyder: "*fragår modtagelsen af pengelån eller andet lån til eje eller af en ydelse, for hvilken der skal svares vederlag".* Denne type underslæb er sjældent anvendt i praksis, og vil derfor kun beskrives kortfattet. Denne bestemmelse skal imidlertid ses som et supplement til bedrageri i strfl's § 279, da der i visse bedragerilignende tilfælde straffes, uden der retsstridigt er fremkaldt, bestyrket eller udnyttet en vildfarelse. Hovedelementet i nr. 2 er en beskyttelse af tilbagebetaling og vederlag for den som har ydet et pengelån eller lån til eje. Den strafbare handling i bestemmelsen er endvidere at nægte at man har modtaget eksempelvis et pengelån eller lån til eje. [67] Et eksempel på dette ses i U 1994.97 V, hvor tiltalte blev fundet skyldig i underslæb, jf. § 278, stk. 1, nr. 2, ved at fragå et lån af 30 tusinde kroner fra afdød, i forbindelse med opgørelse af dødsboet. Denne type underslæb er endvidere fuldbyrdet ved fragåelsen.[68]

Tredje type underslæb findes i strfl's § 279, stk. 1, nr. 3. Denne type underslæb er bedst kendt som *"pengeunderslæb"*[69] og omhandler situationer, hvor man uretmæssigt forbruger penge, som man har fået betroet, og derved opnår økonomisk vinding. Dette fremgår af ordlyden som følger: *"uretmæssig forbruger ham betroede penge, selv om han ikke var forpligtet til at holde disse afsondrede fra sin egen formue."* Pengeunderslæb fuldbyrdes endvidere, når pengene er forbrugt[70] (hvad dette indebærer vil blive behandlet senere i afsnittet). Denne bestemmelse er især vigtig i besvarelsen på specialets problemformulering, hvorfor den også vil blive yderligere behandlet senere.

Denne bestemmelse omhandler forbrug af *"penge"*, hvorfor det er vigtigt at redegøre for hvad dette begreb omfatter. Det må af ordets almindelige betydning og retspraksis utvivlsomt omfatte rede kontanter. Et eksempel på dette er TfK 2010 343/2 Ø, hvor souschef i supermarked tilegnede sig 57 tusinde i kontanter fra supermarkedets pengeskab. *[71]* Derudover ses, det i tilfælde, hvor der bliver misbrugt fuldmagter til at forbruge indestående på bankkonti, jf. TfK 2003.784 Ø, hvor medarbejder på plejehjem anvendte falsk fuldmagt til at hæve penge fra beboernes konti.[72] I denne slags

[66] Ibid., s. spec 674-675
[67] Ibid., s. 676-677
[68] Ibid., s. spec 678
[69] Ibid., s. 672
[70] Ibid., s. 682
[71] Ibid., s. 678
[72] Ibid., s. 680

tilfælde kan der opstå spørgsmål om, hvorvidt sådanne situationer ville blive omfattet af databedrageri fremfor underslæb, hvis der var tale om udnyttet selvbetjeningsfuldmagt. Det fremgår dog ikke af dommen, hvorvidt der også er tale om overførsler via netbank eller om der kun er tale om overførsler foretaget af bankens personale (Læs yderligere herom i det analytiske afsnit). Det er i litteraturen uklart, om begrebet omfatter *"pengerepræsentativer"*, altså fysiske repræsentativer for penge, som eksempelvis omsætningspairer. Det er dog tidligere set, at checks er blevet omfattet, jf. U 1974.243 Ø, hvor leder på et værksted tilegnede sig checks og kontanter som var kommet som betaling fra kunder.[73] Uagtet om dette begreb omfatter "*pengerepræsentativer*", vil disse, hvis de ikke omfattes nok være omfattet af tingsunderslæb, jf. strfl's § 278, stk. nr. 1, da der er tale om "rørlige ting".

Vedrørende de i ovenfornævnte afsnit "*penge*", er det et krav for bestemmelsens anvendelse, at disse skal være "*betroet*" den pågældende.[74] Udtrykket betroet dækker som sagt flere forskellige situationer og optræder også ofte i forbindelse med forbrug i forbindelse med hverv, hvor man har mulighed for at disponerer over pengene. Herunder eksempelvis sit hvert som butiksansat, advokater, revisorer og lignende. I forbindelse med folk som håndterer kontanter, herunder eksempelvis butiksansatte, vil der kunne straffes for underslæb, hvis den butiksansatte tager penge ved en betaling fra en kunde – altså inden pengene f.eks. er lagt i kassen[75], jf. TfK 2006.603 V, hvis der er tale om en kasseansvarlig (med personlig kasse), som tager penge derfra eller hvis man er ansvarlig for kasseafstemning, jf. U 1982.1187/1 V. Modsat vil det være mere nærliggende at dømme for tyveri, jf. strfl's 276 i tilfælde, hvor der er tale om en "*fælles"* kasse.[76]

I forbindelse med anvendelsen af strfl's § 278, stk. 1, nr. 3 skal efter ordlyden, som tidligere nævnt være tale om uretmæssigt forbrug. Her straffes kun det forbrug, som forhindrer personen i at opfylde sin forpligtelse eller skaber en betydelig risiko for at forpligtelsen ikke ville kunne opfyldes. En undtagelse hertil, er hvis der foreligger særlige omstændigheder, hvor man eksempelvis er forpligtet til at holde de betroede penge adskilt fra sin egen formue. Dette vil med andre ord sige, at et forbrug der gør det umuligt for gerningspersonen at stille beløbet til rådighed, når det skal bruges straffes som underslæb efter strfl's § 278, stk.1, nr. 3. Ved en vurdering af hvorvidt et forbrug er uretmæssigt er det derfor ikke tilstrækkeligt at se isoleret på forbruget, men derimod vurderer, hvor

[73] Ibid., s. 678
[74] Ibid., s. 679
[75] Ibid., s. 680
[76] Ibid., s. 680

usikkert det var, at der ville være tilstrækkelige penge til rådighed på tidspunktet, hvor de skulle anvendes.[77]

9. Mandatsvig, jf. Straffelovens § 280

I dette afsnit behandles strfl's § 280 om mandatsvig. Dette er nødvendigt i besvarelsen af problemformuleringen, da forståelsen af bestemmelsen danner ramme for at afdække samspillet mellem bestemmelsen og henholdsvis databedrageri og underslæb.

Mandatsvig er en berigelsesforbrydelse, der er defineret i strfl's § 280. Denne bestemmelse omhandler situationer, hvor en person uberettiget tilegner sig andres formue eller aktiver, som vedkommende har fået betroet adgang til, jf. bestemmelsens ordlyd. Mandatsvig i strfl's § 280 er som nævnt en berigelsesforbrydelse, hvorfor der er krav om berigelsesforsæt. Dette fremgår også af § 278, stk. 1, som lyder: *"§ 280. 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."* Det kræver således, ligesom ved de førnævnte bestemmelser, at gerningspersonen har forsæt til økonomisk vinding og derigennem ligeledes forsæt til tab eller risiko for tab hos modparten. Dette forsæt skal være der på tidspunktet for dispositionen.[78] Mandatsvig fuldbyrdes ved indtrædelse af tabet eller når der er fremkaldt væsentlig risiko for tabet[79]. Ydermere, gør ordlyden af stk. 1: *"så vidt forholdet ikke falder ind under §§ 276-279 a"*, at bestemmelsen får karakter af en opsamlingsbestemmelse for de ovenfor behandlede bestemmelser. Dette vil konkret sige, at bestemmelsen ikke kan anvendes, hvis et forhold falder under det anvendelsesområde, som for strlf's §§ 278, 279 og 279 a, er beskrevet i de tidligere afsnit. Dertil kan mandatsvig ej heller straffes i samstød med førnævnte bestemmelser. Retspraksis viser dog, at man for forskellige forhold i samme retssag straffer for blandt andet mandatsvig og databedrageri, jf. eksempelvis TfK 2017.1158/2 Ø, som behandles yderligere i det analytiske afsnit.

Inden gennemgang af mandsvigs, stk. 1, nr. 1 og 2, er det yderst relevant at nævne, at beskyttelsesinteressen for bestemmelsen omfatter tab, som rammer, eksempelvis et selskab, direkte og omfatter ikke tab, hvor det alene er selskabs kreditorer, som lider et tab eller risikoen herfor. Sidstnævnte forhold vil som udgangspunkt være skyldnersvig, jf. strfl's § 283.[80]

[77] Ibid., s. 681
[78] Ibid., s. 700
[79] Ibid., s. 701
[80] Ibid., s. 699

Mandatsvigsbestemmelsen opdeles i to forskellige forhold første forhold fremgår af bestemmelsens nr. 1, som lyder: *"ved misbrug af en for ham skabt adgang til at handle med retsvirkning for denne..."* For så vidt angår nr. 1, handler det om situationer, hvor gerningspersonen misbruger sin legimitationen i tilfælde, hvor de ikke er forpligtet til at varetage en andens tarv. Dette kan ses i modsætning til bestemmelsens nr. 2, som lyder: *"ved i et formueanliggende, som det påhviler ham at varetage for den anden, at handle mod dennes tarv*. I dette tilfælde er der modsat nr. 1, tale om legimitationsmisbrug, hvor gerningspersonen er forpligtet til at varetage en andens tarv. Heraf er det relevant, at nr. 1 ikke anvendes i tilfælde af overskridelser af stillingsfuldmagter. Der stilles i begge situationer ikke krav til det retsgrundlag, der giver adgang til at handle for modparten. [81]

Som tidligere nævnt er anvendes bestemmelsens nr. 1 i tilfælde, hvor der misbruges legimitation, samt at gerningspersonen ikke er forpligtet til at varetage en andens tarv. Eksempler på dette kan være misbrug af fejlagtigt modtaget blankofuldmagter, altså tilfælde hvor gerningspersoner anvender en fysisk fuldmagt, der ikke er rettet mod dem, til at handle med retsvirkning for fuldmagtsgiver. [82] Andre tilfælde, hvor nr. 1, anvendes er eksempelvis tilfælde som i TfK 2011.737 V, hvor en ansat i en kommune misbrugte sin adgang til at handle på vegne af denne til, at købe en køkkenmaskine hos en catering virksomhed eller TFK 2011.396/2 Ø, hvor gerningspersonen uberettiget betalte benzin til sin egen bil, ved brug af sin arbejdsgivers benzinkort. Sidst nævnte dom omhandler endvidere den uberettigede brug af betalingskort, hvorfor dette ligesom i afsnittet om databedrageri er relevant i forbindelse med mandatsvig. Her er der tidligere nævnt, at der ved misbrug af eget dankort, der er skyld i et overtræk, kan straffes for mandatsvig, jf. strfl's 280, stk. 1, nr. 1," *for så vidt angår den del af overtrækket som er dækket af nets' betalingsgaranti*". Endvidere, er det oftest set at de fleste domme, hvor der foregår uberettiget anvendelse af betalingskort eller lignende, bliver henført til bedrageri eller databedrageri i strfl's §§ 279 og 279 a.

Bestemmelsens nr. 2 anvendes som nævnt i tilfælde, hvor der misbruges legimitation, hvor gerningspersonen er forpligtet til at varetage en andens tarv. Med andre ord taler man ofte om *"misbrug af stilling"*. *"Stilling"* omfatter her blandt andet ledere, advokater, fuldmægtige, bestyrere og værger[83]. Dog vil situationer, eksempelvis ved virksomhedsledere, hvor den handling som er foretaget, utvivlsomt er udenfor vedkommendes beføjelser, ikke være omfattet af mandatsvigsbestemmelsen, i stedet være underslæb. Dog vil sådanne situationer være omfattet, hvis handlingen rent

[81] Ibid., s. 696-697
[82] Ibid., s. 697
[83] Ibid., s. 698

objektivt ville ligge inden for stillingens almindelige beføjelser.[84] Dette kan blandt andet ses i U.1970.838 V, hvor sparekassedirektør hævede kassekredit, der i forvejen var bestemt skulle nedbringes, yderligere. I dette tilfælde burde sparekassedirektøren have indset at han skabte en økonomisk risiko for sparekassen og derfor handlede imod dens tarv. Han blev derfor dømt for mandatsvig, jf. strfl's § 280, stk. 1, nr. 2. Et andet klassisk og kendt eksempel på mandatsvig er U 2008.1607 H (U 2007.1444 Ø), også kendt som Brixtofte- eller Farumsagen, som omhandlede en tidligere borgermester, der i årene 2000-2001 havde gjort at Farum Kommune betalte 9 mio. kroner ekstra til entreprenørforretning som for Farum Kommune skulle bygge en sportshal. Det var Brixtoftes mening, at disse penge, plus 1 mio. kroner fra entreprenøren selv, skulle bruges til sponsorat mellem entreprenøren og en lokal håndboldklub. Brixtofte mente endvidere, at han ikke kunne at an ikke var skyldig i mandatsvig da han havde erklæret sig inhabil, grundet hans tilknytning til håndboldklubben, i forholdet byggesagen. Derudover anførte Brixtofte, at viceborgmesteren havde underskrevet kontrakten om de 9 mio. kroner. Brixtofte blev i flere instanser kendt skyldig for mandatsvig af særlig grov beskaffenhed, jf. strfl's § 280, jf. § 286, stk. 2 overfor kommunen. Her udtalte retten blandt andet at Brixtofte ved at foretage ovenstående handlinger havde misbrugt hans adgang til at handle i et formueanliggende eller på vegne af Farum Kommune, og på denne måde have handlet mod kommunens tarv. Dommen blev fastsat til 2 års fængsel.

10. Analyse

10.1 Bestemmelsernes sammenhæng – en komparativ analyse

For at nå besvarelsen af problemformuleringen er det relevant at lave en komparativ analyse af ovenstående bestemmelser. I denne vil indgå bestemmelserne om bedrageri, databedrageri, underslæb og mandatsvig, jf. strfl's §§ 278, 279 a (herunder 279) og 280, herunder deres forskelle og ligheder. Dog skal det allerede her nævnes, at kun en del af underslæbsbestemmelsens anvendelsesområde vil være relevant for problemformuleringens besvarelse.

Underslæb er som tidligere beskrevet delt op i nr. 1-3, hvor nr. 1 omhandler tilegnelse af fremmed rørlige ting, som er i gerningspersonens varetægt, uden at det falder under strfl's § 277 om ulovlig omgang med hittegods. I nr. 1 er fokus hovedsageligt på "*rørlige ting*", altså fysisk ejendom, som er i gerningspersonens varetægt. Denne type underslæb vil ikke have den store relevans og

[84] Ibid., s. 699

sammenhæng med databedrageri eller mandatsvig, da der i disse ikke indgår et element om at tilegne sig rørlige ting. Det er her mere nærliggende, at tilfælde, der falder udenfor bestemmelsens anvendelsesområde, vil være omfattet af § 276 tyveri, § 277 ulovlig omgang med hittegods eller lignende. Dog kunne denne bestemmelse angiveligt have en tilknytning til databedrageri, hvis man betragtede data og programmer i underslæbsbestemmelsen, som "*rørlige ting*". Det er i retspraksis før nævnt, at data kan være en "*ting*", jf. U 1987.216 Ø, hvor "*Edb-programmer*" blev sidestillet med "*ting*" i strfl's hærværksbestemmelse § 291. Landsretten udtalte endvidere at data i dens bredere form var omfattet af bestemmelsen. Dog er det svært konkret at henføre denne brede fortolkning til tingsunderslæb, da der af 278, stk. 1, nr. 1's ordlyd er krav om at tingen er "*rørlig*" og at dette ikke blev behandlet i retten.

Nr. 2 i underslæbsbestemmelsen omhandler fragåelse af modtagelsen af et pengelån eller andet lån til eje eller af en ydelse, for hvilken der betales vederlag. Denne bestemmelse anvendes sjældent i praksis og adskiller sig markant fra databedrageri eller mandatsvig. Det eneste tænkte eksempel på et overlap ville være et tilfælde, hvor man i forbindelse med sit hverv eller ved at anvende elektronisk databehandling, får oplysninger om at man har lånt f.eks. penge til at forsvinde. Dette er der dog ikke konkret belæg for.

Grundet strfl's § 278, stk. 1, nr. 1 og 2's specifikke anvendelsesområde findes det meget usandsynligt, at der ville kunne ske et overlap med databedrageri eller mandatsvig. Disse bestemmelser vil sandsynligvis kun i tilfælde, hvor der straffes for forskellige forhold komme i forbindelse ved dom.

Alle de nævnte bestemmelser har det tilfælles, at de er berigelsesforbrydelser under kapitel 28 i straffeloven, herunder ligger det subjektive krav om forsæt til uberettiget vinding fra gerningspersonens side (egen eller tredjemands vinding) og et økonomisk tab for modparten. Fælles er også at formuetab i alle bestemmelser skal fortolkes udvidet, så det også omfatter tilfælde, *"hvor vedkommende der har udført den kriminelle handling har indset, at vedkommendes adfærd medførte en vis risiko for tab",* jf. TfK 2008.647 Ø (behandlet i afsnittet om formueforbrydelser). Det gælder ligeledes, at strafferammen for bestemmelserne er den samme og følger af henholdsvis strfl's §§ 285, stk. 1 og 286, stk. 2. Ifølge disse bestemmelser straffes databedrageri (og bedrageri), underslæb og mandatsvig med indtil 1 år og 6 måneders fængsel eller op til 8 års fængsel i tilfælde af forbrydelse af særlig grov beskaffenhed.

For så vidt angår forskellen på de nævnte bestemmelser, adskiller de sig på forskellige måder. Først varierer de i, hvor specifikt indholdet af bestemmelserne er. Her kan det nævnes, at bedrageri

generelt er en meget bred bestemmelse, hvor databedrageri er en mere specifik form for bedrageri, som kun anvendes i forbindelse brug af elektronisk databehandling. Her er underslæb og mandatsvigs ordlyd dog mere sammenlignelig. Pengeunderslæb, jf. strfl's § 278, stk. 1, nr. 3 og mandatsvig, jf. 280, er sammenlignelige, da de begge omhandler forbrydelser, hvor der misbruges en form for tillid til at tilegne sig modpartens formue. Dette adskiller sig fra databedrageri og bedrageri, som ikke kræver sådan et tillidsforhold. Her kan det dog nævnes, at den klare forskel på mandatsvig og pengeunderslæb er, at forbrydelsen for mandatsvigs vedkommende er at handle imod den person, for hvem man skulle varetage et formueanliggende eller misbrug af en på anden måde skabt adgang til at handle med retsvirkning for denne. Modsat indebærer underslæb ikke nødvendigvis et misbrug af tidligere nævnte beføjelser, men blot at gerningspersonen tilegner penge, som er i sin varetægt. Der må endvidere ud fra bestemmelsernes beskrivelse ovenfor kunne udledes, at der er tale om forskellige beskyttelsesinteresser/hensyn. I det der er tale om formueforbrydelser, har bestemmelserne tilfælles, at de alle er til for at beskytte formuer og økonomiske interesser. Underslæb er dog til for at beskytte den tillid, der er forbundet med at betro nogen penge eller andre værdier, mens mandatsvigsbestemmelsen skal sikre, at personer, som har fået en særlig tillid til at handle (med retsvirkning eller i et formueanliggende) på andres vegne, ikke misbruger denne tillid til at skaffe sig eller andre uberettiget vinding. Bestemmelsen om databedrageri må endvidere antages at være til for, at beskytte dataintegritet og tilliden til den elektroniske databehandling. Det er her også vigtigt at sige, som tidligere nævnt, at mandatsvigsbestemmelsen fungerer som en opsamlingsbestemmelse for henholdsvis databedrageri, bedrageri og underslæb, hvilket i princippet ville umuliggøre, at forhold, der falder under disse bestemmelser, vil blive henført under mandatsvig, jf. strfl's § 280. Hertil kan det ydermere nævnes, at databedrageribestemmelsen i strfl's § 279 a, også kan anses som opsamlingsbestemmelse, da forhold som normalt ville falde under de andre bestemmelser, men hvor forbrydelsen sker i forbindelse manipulation (ændring, tilføjelse, sletning eller i øvrigt, jf. bestemmelsens ordlyd) af en databehandling. For at specificere ovenstående og dermed gøre det endnu mere konkret vil specialet nu henledes til analyse af retspraksis. Dette følger af næste afsnit.

10.2 Retspraksis

I nedenstående afsnit vil der ved analyse af retspraksis forsøges, at klarlægge forskelle, ligheder og sammenhænge mellem bestemmelserne om henholdsvis databedrageri, underslæb og mandatsvig, jf. strfl's §§ 279 a, 278 og 280. Det er allerede fastsat i tidligere afsnit at alle domme, der indeholder berigelsesforbrydelser vil have et krav om, at der er forsæt til uberettiget vinding og dermed et

formuetab eller risiko for et sådan hos modparten, hvorfor forsæts- og tabsspørgsmålet ikke vil indgå i analysen af nedenstående domme.

U 1982.1187/1 V:

Denne dom omhandler en person, som lejlighedsvis passede en kasse i et supermarked og i et tidsrum på 1 år og 9 måneder tilegnede sig 70.000 af kassen, ved blandt andet at krediterer tom emballage. Tiltalte blev straffet for pengeunderslæb med fængsel i 4 måneder, jf. strfl's § 285, stk. 1, jf. 278, stk. 1, nr. 3. 1. Denne dom er et klassisk eksempel på pengeunderslæb, hvor tiltalte uretmæssigt har forbrugt betroede penge. Det er dog svært af dommen at tolke, grundet dens manglende detaljering, hvorfor domstolen har dømt for underslæb og ikke tyveri. Men der må sandsynligvis have været tale om en personlig kasse, et tilfælde, hvor tiltalte har taget pengene før de er blevet lagt i kassen eller at tiltalte var ansvarlig for kasseafstemning, hvorfor der har været tale om underslæb, jf. TfK 2006.603, som er omtalt i afsnittet om underslæb. Det interessante ved denne dom er endvidere, at den er af ældre dato. I dag har mange supermarkeder indført foranstaltninger, der gør det vanskeligt at udarbejde kontanter. Med disse systemer, samt den teknologiske udvikling af kassesystemer som i større grad bliver drevet af en computer, vil man angiveligt i dag kunne argumentere for, at en kassemedarbejder, som krediterer en varer og tilegner sig pengene derfra, retsstridigt ændrer eller tilføjer, oplysninger i kassesystemer, der gør det muligt for vedkommende at tilegne sig disse penge. Ud fra denne sondring, vil der muligvis også kunne dømmes for databedrageri, jf. strfl's 279 a i tilfælde, hvor der manipuleres med et computerdrævet kassesystem. Denne antagelse kan endvidere sammenlignes med U 1997.246 Ø, hvor fuldmægtig i andelskasse havde oprettet fiktive obligationshandler via andelskassens IT-system og derved overført penge til sig selv. Tiltalte blev for dette forhold dømt for databedrageri, jf. strfl's 279 a. Dette kan på mange måder sammenlignes, med den fiktive kreditering i det opstillede eksempel. Det vil utvivlsomt, at der tales om underslæb, men derimod databedrageri, hvis systemet anvendes til at krediterer direkte på gerningspersonens eller andres konti. Sådanne tilfælde vil til dels kunne sidestilles med situationer, hvor man uberettiget overfører penge fra en konto til sin egen, som i eksempelvis TfK 2004.539 Ø (se nedenfor for mere), hvor leder i en kommune blev dømt for databedrageri i forbindelse med anvendelsen af kommunens IT-system til at overføre penge til et orkesters konto, hvorefter vedkommende senere hævede beløbet derfra. Ved opsamling af ovenstående kan det konkluderes, at underslæb og databedrageri situationer kan ligne hinanden meget, dog er elementet databehandling vigtigt for at

et forhold som normalt vil være underslæb, bliver til databedrageri. Derudover kan det antages, at udviklingen har gjort, at ting som tidligere har været anset som underslæb, nu (måske) vil blive anset som databedrageri. Her blandt andet tilfælde, hvor anvendelse af kasseapparater er en væsentlig del af forholdet. Derudover antages det samtidig at førnævnte forhold delvist kan sammenlignes med situationer, hvor man uberettiget overfører penge fra en konto til sin egen. I helhed viser denne analyse os, hvad forhold som kan defineres som "misbrug af kreditering" kan blive dømt for. I de konkrete eksempler vil misbrug af kreditering angiveligt blive dømt for enten, underslæb, jf. § 278, stk. 1, nr. 3, når pengene tilegnes fysisk eller databedrageri, jf. § 279 a, hvis pengene tilegnes fysisk, men der indgår manipulation af et computerbaseret kassesystem. En tredje situation, er hvis pengene tilegnes elektronisk og der indgår manipulation af et computerstyret kassesystem. Dette forhold vil utvivlsomt dømmes for databedrageri, jf. § 279 a.

U 1993.667 H:

Denne dom er interessant, da den viser et billede af, hvordan retstilstanden var inden databedragericbestemmelsen reelt blev anvendt i praksis. Desuden er den interessant, fordi henholdsvis byretten og landsretten alene dømmer tiltalte for underslæb, hvor højesteret mener, at tiltalte skal dømmes for både mandatsvig og underslæb. Dommen omhandler en overassistent ved forhenværende Roskilde Amtskommune, som blev anklaget og tiltalt for i en periode på 5 år at have overført 625 tusinde kr. fra amtets konto til sin egen postgirokonto (budgetkonto) og at have tilegnet sig 3.000 kr. som havde været i hendes varetægt. Denne dom var som nævnt gennem flere retsinstanser, hvor tiltalte i byretten først blev dømt for pengeunderslæb af særlig grov beskaffenhed, jf. strfl's 286, stk. 2, jf. 278, stk. 1, nr. 3, for begge forhold. Højesteret vurderede dog, at overførslen fra amtets konto til tiltaltes egen konto, bør være omfattet af mandatsvig, jf. strfl's § 280, stk. 1, nr. 1. Tiltalte blev straffes med fængsel i 1 år og 3 måneder for mandatsvig af særlig grov beskaffenhed, jf. strfl's § 286, stk 2, jf. 280, stk. 1, nr. 1. Årsagen til dette fremgår ikke af dommen, men man kunne forestille sig, at højesteret har ment, at der ikke var tale om betroede midler, men derimod, at tiltalte havde misbrugt sit mandat, altså den skabte adgang til at handle med retsvirkning for Amtskommune. Det skal her siges, at man som ansat leder i en offentlig institution, må antages at have fået en særlig tillid til at handle på kommunes vegne, hvorfor det i situationen er mere nærliggende, at henfører sådanne forhold under mandatsvig. Man kan dog undre sig over, hvorfor højesteret på dette tidspunkt ikke anvender strfl's § 279 a om databedrageri. Spørgsmålet herom er desuden ikke behandlet af

domstolen, men hvis overførslen var sket elektronisk og at der derfor må have indgået en form for manipulation af en elektronisk databehandling, ville man nemt kunne argumentere for anvendelse af databedrageribestemmelsen frem for mandatsvig. Denne antagelse vil også kunne støttes i, TfK 2004.539 Ø, som kort er beskrevet ovenfor, *"hvor leder i en kommune blev dømt for databedrageri i forbindelse med anvendelsen af kommunens IT-system til at overføre penge til et orkesters konto, hvorefter vedkommende senere hævede beløbet derfra"*. Her er der i princippet også tale, om en person der har mandat til at handle med retsvirkning for en kommune. Ifølge tiltalen lød det, at lederen adskillige gange havde retsstridigt ændret, tilføjet eller slettet oplysninger til elektronisk databehandling eller i øvrig søgt at påvirke resultatet af en sådan databehandling, ved at anvende kommunens IT-baserede betalingssystem, til brug i sociale sager, til at overfører i alt 3,8 mio. kroner. til en konto han selv havde oprettet. Denne tiltale ville i princippet kunne overføres (næsten) direkte til U 1993.667 H, hvis der var i dommen, var fakta der pegede i retning af, at der også i dette tilfælde var brugt et IT-baseret system til at foretage overførslerne. Ud fra dette ser det angiveligt ud til, at der tidligere – også efter databedrageribestemmelsens indførsel i 1985, er blevet dømt for mandatsvig, i forhold der muligvis også kunne være dømt for databedrageri. Dette er endvidere sket, selvom mandatsvig skulle have karakter af en opsamlingsbestemmelse, hvor der ikke kan dømmes for forhold, der kan være blandt andet databedrageri, jf. § 280's ordlyd *"så vidt forholdet ikke falder ind under §§ 276-279 a"*. Ovenstående viser også, hvor kompliceret der er at skelne mellem henholdsvis underslæb og mandatsvig. Dette ses i det at både byretten og landsretten først dømte for underslæb, før højesteret ændrede resultatet til mandatsvig i U 1993.667 H. Dette indikerer et overlap af bestemmelsernes anvendelsesområde.

U 2001.2110 V:

I denne dom blev der modsat, tidligere nævnte U 1993.667 H, ændret tiltale fra mandatsvig til underslæb. Dommen omhandler en person, der havde fået adgang til at disponerer over en andens konto. I forbindelse med denne ret til disponering, overførte vedkommende henholdsvis 13 og 288 tusinde kroner til sin egen konto med modpartens samtykke. Disse penge skulle anvendes til afholdes af udgifter for modparten, samt opgørelse af modpartens mors dødsbo. Her blev der i første anklageskrift rejst tiltale for mandatsvig, jf. strfl's § 280, ved at tiltalte "*fra L's konto…, hvorpå han havde adgang til at disponere, at have overført henholdsvis 13.209,32 og 288.000,00 kr. til sin egen konto… med tilsvarende formuetab eller risiko herfor til følge for L"*. Ud fra denne

udlægning er det klart, at det citerede forhold må falde under anvendelsesområdet for mandatsvig, jf. 280, stk. 1, nr. 2, hvor der er tale om misbrug af legimitation, hvor gerningspersonen er forpligtet til at varetage en andens tarv. Dog er problemet angiveligt her, at pengene ved samtykke var blevet betroet og allerede var i tiltaltes besiddelse. Den kriminelle handling må i tilfældet her ikke være overførslen af pengene, men det uberettigede forbrug heraf efter de var indbetalt på kontoen. Dette er blot en antagelse, da dette ikke konkret beskrives i dommen. Denne antagelse støttes endvidere i anklagemyndighedens ændrede anklageskrift, hvor tiltalen modsat tidligere lød: *"straffelovens § 278, stk. 1, nr. 3, underslæb, ved i perioden fra den 3. marts 1998 og til dags dato, for derigennem at skaffe sig uberettiget vinding, uretmæssigt at have tilegnet sig ca. 100.000 kr. af de 302.483,15 kr., som med L's samtykke var overført til tiltaltes konto nr. i BG-Bank med henblik på at afholde udgifter for L og opgøre boet efter M"*. Denne dom er i viser i sin helhed, hvornår noget er underslæb i stedet for mandatsvig. I dette tilfælde var der tale om penge, der var betroet, hvorfor § 278, stk. 1, nr. 3 fandt anvendelse frem for mandatsvig efter § 280, stk. 1, nr. 2. Principielt ville forholdet, som i det første anklageskrift, antages at være mandatsvig, hvis tiltalte ikke havde samtykke til at overføre pengene. Dette forhold ville også kunne dømmes for databedrageri, hvis overførslen er foretaget uden samtykke ved at manipulerer en databehandling, eksempelvis en uberettiget overførsel fra modpartens netbank.

10.2.1 Kombinationsdomme

I retspraksis er der eksempler på kombinationsdomme, altså domme, hvor der indgår flere forhold, som straffes forskelligt. Relevant for specialets problemformulering af henholdsvis TFK 2010.785 V og TfK 2017.1158/2, som er kombinationsdomme der indeholder overtrædelse af strfl's §§ 278, 279 a og 280. Der vil ydermere indgå andet retspraksis som sammenligningsgrundlag. Disse vil blive analyseret nedenfor.

TfK 2010.785 V (kombinationsdom 1):

I denne dom blev tiltalte, som var bogholder, dømt for overtrædelse af strfl's § 297 a, jf. § 286, stk. 2, databedrageri af særlig grov beskaffenhed, samt underslæb, jf. STRFL § 278, stk. 1, nr. 3. Straffen blev fastsat til fængsel i 1 år og 6 måneder. Tiltalte havde i årene 2002-2008 uberettiget tilegnet sig lidt under en mio. kroner fra sin arbejdsgiver. Dette var sket ved, at tiltalte havde overført ca.

857 tusinde kroner fra arbejdsgivernes bankkonti til sin egen konto og udstedt og hævet uretmæssigt checks for omkring 137 tusinde kroner. Endvidere havde tiltalte udstedt og hævet checks for 6.500 kroner i hans egenskab som bogholder for et varmeselskab. Her henførtes forholdet om overførslen af de 857 kroner fra firmaernes bankkonti, under databedrageri af særlig grov beskaffenhed, jf. strfl's § 279 a, jf. § 286, stk. 2. Dette skyldes at der var tale om elektroniske overførsler. Udover dette henførtes begge forhold om udstedelse og hævning af checks under pengeunderslæb, jf. § 278, stk. 1, nr. 3. Beslutningstagningen om, hvorfor sidste de sidste forhold bliver henført under pengeunderslæb, er ikke angivet i dommen. Dog kan årsagen muligvis være, at der er tale om betroede midler som udstedes som checks og derefter forbruges af revisoren. Med hensyn til første forhold dømmes der som sagt for databedrageri. Dette er dog ikke tilfældet i TfK 2016.779 Ø, hvilket er interessant. I denne dom havde revisor, som var havde betroet adgang til modpartens konto uberettiget udstedet checks for ca. 168 tusinde kroner og hævet dem, samt overført ca. 237 tusinde kroner til konti ejet af tredjemænd, hvorefter han brugte en del af pengene til rent private formål. Denne dom er fra 2016, og man må derfor antage at pengene er blevet overført via en selvbetjeningsløsning, som eksempelvis en netbank. Dette gør at disse to domme er stærkt sammenlignelige og viser i sin helhed, at forhold, hvor en revisor/bogholder har adgang til en virksomheds netbank kan være både databedrageri og underslæb. Det er svært ud fra ovenstående at sige hvad årsagen til forskellen reelt er, da en bogholder og en revisor grovest talt har samme arbejdsområde. Til sidst bør det nævnes, at TfK 2010.785 V er et eksempel, hvor en adgang til betroede midler kan udløse to forskellige kriminelle handlinger, i dette tilfælde underslæb (checks) og databedrageri (overførsler).

TfK 2014.577 V:
Denne dom er i lang udstrækning det samme som de to ovenstående, henholdsvis TfK 2010.785 V og TfK 2016.779 Ø. Tiltalte var i dommen bogholder for et varmeselskab, hvor hun havde tilegnet sig 4,8 mio. kroner, ved til dels at overføre beløb til sin egne, ægtefælles eller ægtefælles virksomheds konti. Tiltalte blev dømt efter strfl's § 278, stk. 1, nr. 3, jf. § 286, stk. 2 for underslæb af særlig grov beskaffenhed. Straffen blev desuden fastsat til 2 års og 6 måneders fængsel. I denne sag er der endvidere også ting der kunne argumentere for databedrageri frem for underslæb. Det fremgår af sagens faktum at tiltalte har udtalt at hun overførte pengene ved brug af NEM-id og netbank. Dette taler i stor grad for at der kan tales om databedrageri. Der er i dommen dog taget stilling om hvorvidt, der kunne være tale om databedrageri. En ting der gør denn.39e dom interessant, fremgår af dommens bilag 1.8.b og lyder:*"... dankorthævninger, har tiltalte forklaret, at det kun er hende,*

der har haft dankort til kontoen. Foreholdt at der i en uge i juli 2005 blev hævet 11.554 kr., i en uge i 2006 blev hævet 9.314 kr., og at der i 2010 og 2011 blev brugt mellem 11.000 og 13.000 kr. om ugen…". Hvis denne dom sammensættes afsnittet om databedrageri, hvor der i vidt omfang er blevet behandlet den uberettigede brug af andres betalingskort, vil det kunne ses at det er ualmindeligt at man ved denne form for kriminalitet bliver dømt for underslæb. Hævningerne i denne dom minder mest om dem som er nævnt i den tidligere dom, er U 2014.1688 V, hvor stjålne hævekort blev anvendt til at hæve adskillige beløber. Den væsentlige forskel på disse kan dog antages at være det faktum at tiltalte i nærværende sag normalt har adgang til dankortet i forbindelse med hendes hverv, og at dankortene i U 2014.1668 V er stjålet. Dog kan der stadig tales for at anvendelsen af varmeselskabets dankort kan være databedrageri, jf. strfl's § 279 a. Denne antagelse beror på den automatiske proces, der sker ved anvendelse af dankortet i en hæveautomat. Det skal dog her siges, at anvendelse af dankortet i en butik angiveligt vil være omfattet af bedrageri, jf. strfl's 279, da der her ville ske vildledelse af en person. Der er dog ikke nok information, for så vidt angår overførslerne, til at konkludere dette fuldt ud. Endvidere kan det siges, at ovenstående forhold måske også ville være databedrageri, hvis hævningerne var sket online, jf. TfK 2022.173 Ø, om frisørlærlingen, der anvendte sin arbejdsgivers hævekort til privatkøb. Disse domme har dog en vis forskel i det, at dankortet som frisørlærlingen anvender er et kort, der normalt ikke er i hendes besiddelse, mens bogholderen for varmeselskabet anvender et kort hun normalt har adgang til. Ud fra denne betragtning ville sådanne eksempler angiveligt både kunne være pengeunderslæb, jf. strfl's § 278, stk. 1, nr. 3 og databedrageri fordi der tilegnes penge gennem en automatiseret proces, her hævning i pengeautomater.

TfK 2016.1218 V:

I denne dom havde tiltalte, i forbindelse med sin position som daglig leder i administrationen i en virksomhed, fra januar til oktober 2012, overført i alt 1,1 mio. kroner fra virksomhedens bankkonto, via netbank, som han havde adgang til, til sin egen konto. Derudover havde tiltalte oprettet falske oplysninger om arbejdstider, hvorefter de blev udbetalt til en person som uberettiget fik udbetalt 147 tusinde kroner. Derudover lavede han falske oplysninger om arbejdstimer, hvilket resulterede i uretmæssige lønudbetalinger til en person på 147.566 kr. Disse penge blev derefter overført tilbage til sin egen konto. Tiltalte blev i byretten, dømt for mandatsvig af særlig grov beskaffenhed, jf. strfl's 286, stk. 2, jf. § 280, stk. 1, nr. 1, for at anvende den adgang han havde til, at disponere på

virksomhedens konto, til at skaffe sig økonomisk vinding. Straffen blev fastsat til 1 år og 6 måneders fængsel. Denne sag ligner til forveksling sagerne ovenfor, TfK 2016.779 Ø, TfK 2010.785 V og TfK2014.577 V, hvor der også er eller antages at være foretaget transaktioner via netbank. I denne sag er der endvidere, som i de tidligere domme tale om en person, der har adgang til at administrerer en konto for en virksomhed. Dog er forskellen nok her, at tiltalte i TfK 2016.1218 V overfor de andre ikke utvivlsomt at bogholdere eller revisorer må siges, at have en mere betroet adgang, som led i deres stilling, til penge end en administrativ leder i en virksomhed. I forhenværende blev følgende udsagn nævnt: *"mandatsvigsbestemmelsen fungerer som en opsamlingsbestemmelse for henholdsvis databedrageri, bedrageri og underslæb, hvilket i princippet ville umuliggøre, at forhold, der falder under disse bestemmelser, vil blive henført under mandatsvig, jf. strfl's § 280"*. I dette tilfælde ser vi en dom, som muligvis fragår bestemmelsens ordlyd for så vidt, angår ordene *"så vidt forholdet ikke falder ind under §§ 276-279 a"*.

TfK 2017.1158/2 Ø (kombinationsdom 2):
I denne dom blev tiltalte, som var økonomisk værge for modparten, tiltalt for databedrageri, underslæb og mandatsvig af særlig grov beskaffenhed, jf. STRFL's § 279 a, § 278, stk. 1 nr. 3 og § 280, alt, jf. 286. Tiltalte havde som økonomisk værge overført samlet 8,7 mio. kroner fra konto til sin egen eller andres konti til brug for sine egne private indkøb. Endvidere havde T forfalsket sin fødsels- og dåbsattest og anført F som sin mor, for derefter at fremlægge denne til bobestyreren ved F's død. Straffen blev grundet dens særlige grove beskaffenhed fastsat til 4 års fængsel. Dette skyldes blandt andet tiltaltes betroede stilling som værge, *"overførslernes varighed og systematiske karakter og beløbets størrelse".* Denne dom er et unikt eksempel på, at samtlige af specialets nærværende bestemmelser kommer i samspil med hinanden. Hvad der blandt andet er interessant i dommen, er at byretten anfører samme forhold, nemlig i forbindelse med tiltale i for alle bestemmelser. De nævner i tiltalen, at forholdet bør være; Underslæb, jf. strfl's § 278, stk. 1, da der er tale om uretmæssig tilegnelse af betroede penge. Databedrageri, jf. strfl's § 279 a, stk. 1, da der retsstridigt er påvirket udfaldet af en databehandling, ved mange gange, via netbank at overfører penge. Samt mandatsvig, jf. strfl's § 280, da der blev misbrugt en adgang til at handle med retsvirkning. Landsretten opdelte dog forholdet i to forhold efter anklagemyndigheden præciserede, at 625 tusinde kroner, af de ca. 8,7 mio. kr. ikke var overført elektronisk, men af ansatte i banken. Landsretten dømte i sagen tiltalte for underslæb for så vidt angår de 625 tusinde kroner, og databedrageri for de elektronisk overførte

penge. Det må endvidere, selvom det ikke fremgår af dommen, at tiltalen for mandatsvig frafalder, da den ikke kan finde anvendelse i tilfælde, hvor databedrageri eller underslæb finder anvendelse.

11. Konklusion

Som følge af specialets problemstilling var målet at undersøge samspillet mellem databedrageri i strfl's § 279 a om databedrageri og strfl's §§ 278 og 280 om underslæb og mandatsvig. Dette søges gjort ved anvendelse af den retsdogmatiske metode, som går ud på at analysere og beskrive gældende ret. Disse bestemmelser er med deres ordlyd citeret i de beskrivende afsnit. For at kunne gøre dette skulle bestemmelsernes anvendelsesområde, samt de generelle krav for formueforbrydelser gennemgås. Som fælles træk er de nævnte bestemmelser formueforbrydelser som hører under strfl's kapitel 28. De har med deres karakter af "berigelsesforbrydelse" krav om forsæt til uberettiget vinding – egen eller tredjemands – og derved et økonomisk tab for modparten. Fælles for disse bestemmelser er at "tab" fortolkes udvidet, så det også gælder situationer, hvor der kun er risiko for tab, jf. TfK 2008.647. Dog har databedrageri i § 279 a's et fremrykket fuldbyrdelsesmoment, hvilket gør det umuligt at anvende bestemmelsen uden, der er sket formuetab. Databedrageri fuldbyrdes desuden direkte ved manipulationen. Det forventes altså, at der ikke skal gøres mere for at opnå økonomisk vinding. Bestemmelserne har endvidere samme strafferamme. Denne findes i henholdsvis strfl's § 285, stk. 1, *" fængsel indtil 1 år og 6 måneder*" og i tilfælde af forbrydelse af særlig grov beskaffenhed i strfl's § 286, stk. 2 *"fængsel indtil 8 år"*. Det kan ses i det for specialet anvendte praksis, at der oftest straffes for særlig grov beskaffenhed, men at domstolen derimod er tøvende med at give straffe over 1 år og 6 måneder. Dette kan blandt andet støttes i Brixtofte-sagen, hvor han alene blev straffet med 2 års fængsel. Derudover er der intet der indikerer, at strafferammen for bestemmelserne differentierer i praksis.

Databedrageri, jf. strfl's § 279 a, konkluderes, at omfatte retsstridige ændringer, tilføjelser eller sletninger (manipulation) af data eller programmer i elektronisk databehandling, eller andre måder, hvorpå man forsøger at påvirke resultatet af sådan databehandling. For databedrageri er der, krav om anvendelsen af et "anlæg" til brug for manipulerer data eller programmer. Et sådant anlæg kunne være computere, smartphones, eller generelt anden teknologi, hvori der ligger automatiserede processer. Databedrageri dækker blandt over, situationer, hvor der uberettiget overføres penge via andres netbank, jf. TfK 2010.785 V og hvor der uberettiget (tyveri af fysiske betalingskort eller oplysninger på kort) anvendes andres betalingskort eller mobilbetalingstjeneste, hvor disse er

tilknyttet. Databedrageri adskiller sig fra bedrageri ved, at der i forbindelse med bedrageri kræves en vildfarelse af en fysisk person, som deraf bliver bestemt til en handling eller undladelse. Disse bestemmelser kan nemt forveksles i forbindelse med anvendelse af hævekort, da der i nogle tilfælde kan være mennesker der konkret forholder sig til eksempelvis betalinger.

Underslæb, jf. strfl's § 278 indeholder 3 forskellige typer underslæb. Tingsunderslæb, jf. § 278, stk. 1, nr. 1, fragåelse af at have modtaget lån eller ydelser, jf. nr. 2 og pengeunderslæb, jf. nr. 3. I forbindelse med første del af analysen er det blevet klarlagt ikke alle typer underslæb er sammenlignelige med databedrageri- og mandatsvigsbestemmelserne. Det må ud fra den komparative analyse af bestemmelserne antages, at underslæb efter strfl's § 278, stk. 1, nr. 1 (tingsunderslæb), har hovedfokus på at tilegne sig fysisk ejendom/rørlige ting. Der blev endvidere kort diskuteret, om hvorvidt data kunne være en "ting" på samme måde, som den har været det ved blandt andet hærværk, jf. U 1987.216 Ø, men dette tingsbegrebet må anses, at skulle bruges i tilfælde, hvor ordlyden af en bestemmelse kun er "ting" og ikke "rørlige ting". Tingsunderslæb må derfor antages ikke at kunne have et samspil med databedrageri, medmindre der straffes for to vidt forskellige forhold. Der er endvidere heller ikke grobund for at samspil med mandatsvig, da dennes beskyttelsesinteresse ligger i *"at personer, som har fået en særlig tillid til at handle på andres vegne, ikke misbruger denne tillid til at skaffe sig eller andre uberettiget vinding."* Denne særlige tillid kan desuden komme til udtryk ved at kunne handle med retsvirkning for eller i et formueanlæggende på vegne af andre. Det må ydermere, antages at underslæb efter strfl's § 279, stk. 1, nr. 2, som angår *"fragåelse af modtagelsen af et pengelån eller andet lån til eje eller af en ydelse, for hvilken der betales vederlag."* Har så specifik en ordlyd, der gør at den adskiller sig markant fra databedrageri og mandatsvig. Desuden anvendes den yderst sjældent, og kun i tænkte eksempler ville den kunne have et snævert samspil med databedrageri og mandatsvig. Denne bestemmelse vil sandsynligvis, som tingsunderslæb, kun i forbindelse med straf for forskellige forhold komme i forbindelse med databedrageri eller mandatsvig. Den tilbagestående underslæbstype "pengeunderslæb", jf. 278, stk. 1, nr. 3, er endvidere mere sammenlignede med de for specialet relevante bestemmelser. Denne bestemmelse angår retsstridigt forbrug af betroede penge. Kravene for bestemmelsens anvendelse er at der skal være sket et forbrug. Dette indebærer, at den anklagede har brugt penge på en måde, der enten forhindrer dem i at opfylde deres forpligtelser eller skaber en betydelig risiko for, at forpligtelsen ikke vil kunne opfyldes. Der skal endvidere være tale om betroede penge, hvorfor gerningspersonen skal have pengene i hans varetægt inden tilegnelsen. Det er uklart, hvad der omfattes at begrebet "penge", men det må uomtvisteligt handle om rede kontakter, samt indestående på bankkonti. Dog er der eksempler, hvor

pengerepræsentativer også er blevet omfattet. Dette ses blandt andet ved checks, jf. vs. fysiske repræsentanter for penge, såsom omsætningspapirer. Der er dog eksempler i retspraksis, hvor checks er blevet omfattet af begrebet penge - se U 1974.243 Ø og TfK 2010.785 V. Eksempler på pengeunderslæb, jf. strfl's § 278, stk. 1, nr. 3, kan være leder som tilegner sig penge fra virksomhedens pengeskab, jf. TfK 2010 343/2 Ø, anvendelse af fuldmagt til uberettiget at hæve penge på fuldmagtsgivers konto, jf. TfK 2003.784 Ø, tilegnelse af betalinger fra kunder (hvor pengene ikke bliver lagt væk – i kasse eller lignende), jf. U 1974.243 Ø og TfK 2006.603 V eller kasseansvarlige, med personlig kasse, som tilegner sig penge derfra, jf. U 1982.1187/V.

Mandatsvig, jf. strfl's § 280, kan anses som en opsamlingsbestemmelse for databedrageri og underslæb, jf. ordlyden af, stk. 1:*"så vidt forholdet ikke falder ind under §§ 276-279 a"*. Dette vil i princippet sige, at bestemmelsen ikke kan anvendes, hvis et forhold falder under det anvendelsesområde, som for strfl's §§ 278, 279 a. Dette er måske blevet modbevist i TfK 2016.1218 V, hvor der straffes for mandatsvig for et forhold, der muligvis også kunne straffes for databedrageri – her uberettiget overførsel via. Netbank. Bestemmelsen kan deles op i to forskellige typer forhold. Nr. 1 som omhandler, situationer om misbrug af adgang til at handle med retsvirkning for andre og Nr. 2 som omhandler, situationer hvor man ved i et formueanliggende, som det påhviler en at varetage for den anden, at handle mod dennes tarv. I dette tilfælde er der modsat nr. 1, tale om legimitationsmisbrug, hvor gerningspersonen er forpligtet til at varetage en andens tarv. Heraf er det relevant, at nr. 1 ikke anvendes i tilfælde af overskridelser af stillingsfuldmagter – og der stilles ikke krav til det retsgrundlag, der giver adgang til at handle på vegne af modparten. Mandatsvig kan endvidere være tilfælde, hvor kommunalt ansatte misbruger deres stilling til vinding til sig selv eller andre i form af aktiver eller penge aktiver på kommunens regning, jf. TfK 2011.737 V og U 2008.1607 H (Brixtofte-sagen). Ydermere situationer, hvor man har fået mandat til arbejdsrelateret brug af betalingskort, benzinkort m.v. af sin arbejdsgiver, jf. TfK 2011.396/2 Ø.

I forbindelse med sammenligningen af ovenstående bestemmelser, der i den komparative analyse kommet frem til at bestemmelserne varierer i, hvor specifikke de er i deres indhold. Her kan det ydermere siges, at databedrageri er en mere specifik form for bedrageri som kun anvendes i forbindelse brug af elektronisk databehandling. Denne er efter dens ordlyd svær at sammenligne med underslæb og mandatsvig, men grundet dens beskedne krav om den elektroniske databehandling ville den i princippet kunne bruges både tilfælde af underslæb og mandatsvig, hvis dette er opfyldt. Det konkluderes her, at pengeunderslæb og mandatsvig er langt mere sammenlignelige. Der er i begge tilfælde tale om bestemmelser, hvor der bliver misbrugt en tillid, hvilket også adskiller dem fra

databedrageribestemmelsen, som ikke har dette element. Ved underslæb kontra mandatsvig kan det siges at underslæb ikke kræver misbrug af en skabt adgang eller formue anlæggende, som vedkommende varetager. Underslæb kræver blot tilegnelse af noget man har i sin varetægt. Ved en konkret sammenligning af bestemmelsernes beskrivelse er der udledt forskellige beskyttelsesinteresser. Fælles for alle bestemmelser er at beskytte mod formuetab. Disse beskyttelsesinteresser er tidligere beskrevet som *"Underslæb er … til for at beskytte den tillid, der er forbundet med at betro nogen penge eller andre værdier, mens mandatsvigsbestemmelsen skal sikre, at personer, som har fået en særlig tillid til at handle på andres vegne, ikke misbruger denne tillid til at skaffe sig eller andre uberettiget vinding. Bestemmelsen om databedrageri må endvidere antages at være til for at beskytte dataintegritet og tilliden til den elektroniske databehandling."* Disse beskyttelsesinteresser kan antages at have betydning for, hvilke bestemmelser domstolen henfører forskellige forhold under. Der er dog ikke konkret belæg for dette udsagn. Endvidere ser man på kryds af den komparative analyse og analysen af retspraksis, at der ofte er en meget tæt tilknytning mellem bestemmelserne. Der er blandt andet tilfælde, hvor forskellige bestemmelser bruges for noget der ligner det samme forhold. Dette er f.eks. tilfældet i TfK 2016.779 Ø, TfK 2010.785 V, TfK 2014.577 V og TfK 2016.1218 V, der alle omhandler uberettigede overførsler til egne eller andres konti. Ved disse domme er det interessante blandt andet er der straffes for henholdsvis databedrageri, underslæb og mandatsvig for dette samme forhold. Der fremgår ikke af dommene, hvorfor der ikke bliver overvejet andre bestemmelser. Men det må være sikkert, at disse tilfælde alle ville kunne straffes for databedrageri, hvis overførslerne er sket via netbank, hvilket de sandsynligvis er – og der på den måde indgår elektronisk databehandling. Der må desuden i forbindelse med U 1982.1187/1 V, konkluderes at der før indførslen af databedrageri bestemmelsen har været retspraksis, som den dag i dag, måske som følge af den teknologiske udvikling ville blive betragtet som databedrageri. Dommen omhandler tilegnelse fra penge fra et kassesystem ved falsk kreditering. I dag ville disse tilfælde angiveligt kunne blive betragtet som databedrageri, da mange kassesystemer i dag er computerstyrede, og det derfor ville kræve manipulation af dette system, for at foretage falsk kreditering. Det må vurderes ud fra analysen sådanne falske krediteringer kan dømmes for, underslæb, jf. § 278, stk. 1, nr. 3, når pengene tilegnes fysisk eller databedrageri, jf. § 279 a, hvis pengene tilegnes fysisk, men der indgår manipulation af et computerbaseret kassesystem. Der kunne i denne situation også argumenteres, at den tilegnelse kunne være tyveri eller underslæb alt efter omstændighederne, hvorfor man kunne straffe i samstød. Herunder ville kreditering til egen konto med sikkerhed være databedrageri, jf. § 279 a. I forbindelse besvarelsen af opgavens problemformulering er det endvidere

relevant at tage fat i situationer, hvor hævekort eller lignende betalingsmidler er blevet anvendt uberettiget. I sådanne situationer er der igen sammenfald mellem databedrageri, mandatsvig og pengeunderslæb. TfK 2014.577 V viser os at den uberettigede brug af hævekort godt kan dømmes for underslæb, også selvom pengene er hævet i en automat (databehandling). Domstolen nævner endvidere slet ikke databedrageri som en mulighed. Dette gælder som udgangspunkt for alle de domme, der er behandlet som kunne være databedrageri. TfK 2011.396/Ø, hvor tiltalte er dømt for mandatsvig, for at udnytte det mandat han har fået mandat til arbejdsrelateret brug af betalingskort. Her er der tale om et benzinkort, der anvendes på en ubemandet station, hvorfor der også kunne være tale om databedrageri. Til sidst kan det konkluderes, at der på mange måder findes situationer, hvor anvendelsesområdet for både mandatsvig, databedrageri og pengeunderslæb overlapper. Dette er blandt andet set i situationer med uberettigede hævninger fra netbank eller uberettiget brug af betalingskort. Der ses endvidere eksempler på, at der i samme dom forsøges, at dømme for flere bestemmelser – dog for flere forskellige forhold. Et relevant område, som også omhandler uberettigede hævninger, er situationen, hvor man eventuelt trækker over på nettet og overstiger nets' betalingsgaranti, her ville der angiveligt blive straffet for mandatsvig, jf. strfl's § 280, stk. 1, nr. 1, for så vidt angår beløbet, der er dækket at betaling garantien fra nets og databedrageri, jf. § 279 a.

Det er endvidere set, i TfK 2017.1158/2 Ø, at man har forsøgt at dømme for underslæb og databedrageri i samstød. Dog blev disse forhold opdelt i en fysisk hævning og en elektronisk hævning, hvor der efter de to forhold blev dømt for henholdsvis pengeunderslæb, jf. § 278, stk. 1, nr. 3 og databedrageri, jf. strfl's § 279 a. Det skal her tilføjes, at det vil være højest usandsynligt at straffe for mandatsvig og databedrageri, da mandatsvig i princippet ikke må anvendes, hvis databedrageri kan. Det må ydermere konkluderes, at databedrageri nu sammenlignet med årene efter dens indførsel bliver brugt oftere. Der er her tidligere straffes for mandatsvig i sagen, U 1993.667 H, hvor der kan antages at være tale om netbank overførsler. Denne dom er fra 1993, og det viser i sin helhed, sammen med det beskedne antal ældre databedrageri domme, at man ikke før århundredeskiftet rigtigt fik øje på databedrageribestemmelsen. Det kan dog ses, at der fortsat bliver henført forhold under mandatsvig eller underslæb, som principielt også kunne henføres under databedrageri, jf. strfl's 279 a, fordi der en eller anden måde indgår manipulation af en databehandling. Det er dog i praksis underordnet, hvor den reelle grænse går mellem bestemmelserne. Dette skyldes den, tidligere nævnte, fælles strafferamme.

12. Diskussion

Ud fra ovenstående vil det diskuteres om ordlyden af databedrageri i sig helhed er for bred. Det tyder på at der på sin vis er valgfrihed hos domstolen i forhold til at vælge om et forhold falder under databedrageri. Dette kan skyldes dens nære tilknytning til henholdsvis underslæb, bedrageri og mandatsvig. Dette åbner endvidere for en diskussion om, hvorvidt den danske straffelovgivning til tider kan være for ukonkret, og måske også forældet på det cyberkriminelle område. Til sammenligning vil der her bruges den tyske straffelov - "Strafgesetzbuch". Årsagen til valget af land er at Tyskland på mange måder må anses, at mange skridt bag Danmark, når det gælder digitalisering. Dog kan det tyde på, at Tyskland har været mere progressiv i med hensyn til at vedtage straffelovsbestemmelser, der er mere specifikke, specielt på det cyberkriminelle område. Som eksempel kan det nævnes, at der i den tyske straffelovgivning er selvstændige bestemmelser for phishing og dataspionage – disse findes i Strafgesetzbuch §§ 202 a og 202 b. Phishing vil i dansk sammenhæng indgå i bestemmelsen om databedrageri. Tyskland har ydermere indsat yderligere foranstaltninger for phishing i 202 c, hvor man kan straffes forberedelse til phishing eller dataspionage. Det er svært fuldt at konkluderer, hvorvidt forberedelse til databedrageri vil blive straffet. Der vil måske i angiveligt i denne sammenhæng straffes for forberedelse til databedrageri, jf. strfl's § 21. Denne bestemmelse omhandler *"Handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse, straffes, når denne ikke fuldbyrdes, som forsøg."*. For dataspionages vedkommende vil dette angiveligt i dansk regi ramme den danske straffelovs § 263, der lyder *"Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem."*. Her er beskyttelsesobjektet data i et bredere perspektiv end blot spionage. Der kunne eventuelt også tales om brug af databedrageribestemmelsen i tilfælde, hvor der sker dataspionage med berigelsesforsæt. Det kunne eksempelvis være spionage, hvor det er tiltænkt at sælge oplysningerne videre. Disse to tyske bestemmelser er blot et fåtal af bestemmelser, der har et langt mere specifikt end de danske. Udover ovenstående har den tyske straffelov også en bestemmelse vedrørende computer-sabotage, altså datahærværk. Forskellen her er, at man i Danmark har valgt at fortolke udvidet på begrebet "ting", jf. U 1987.216 Ø, så det omfatter data, hvorfor datahærværk i Danmark straffes den almindelige hærværkbestemmelse i strfl § 291. Fordelen ved, at de tyske bestemmelser er så specifikke, er for det første, at lovgiver ikke er i tvivl om, hvilke forhold der kan straffes for hvad. Der kan endvidere argumenteres for at tydeligheden i hvad der kan straffes for, forøger retssikkerheden og det kan på baggrund af dette måske argumenteres for at det vil være en forbedring af den danske straffelov at have mere specifikke

bestemmelser på området for cyberkriminalitet. På den anden side kan det også argumenteres, at en mere detaljeret og specifik lovgivning ikke nødvendigvis er bedre, da det kan føre til større kompleksitet og bureaukrati. Det kan her argumenteres for vigtigheden i at finde den rette balance mellem detaljer og enkelhed i straffelovgivningen for at sikre effektiv beskyttelse mod datakriminalitet, men også samtidig gøre det lettere for virksomheder og borgere at overholde loven. Samlet set er det svært, at konkluderer, om den danske straffelovgivning er forældet set i sammenhæng med den tyske. Dette skyldes de to landes forskellige tilgange til regulering af cyberkriminalitet. Det kan desuden her siges, at begge lande ikke har indført straf for cybermobning, som er et generelt stigende problem. Endvidere er dansk straffelovgivning er præget af ”opsamlingsbestemmelser” og udvidede fortolkninger, hvilket på sin vis er en god ting, da brug af ny teknologi eller metoder på denne måde ikke vil falde udenfor straffelovens anvendelsesområde.

13. Kildeliste

Kildehenvisning som set i specialets brødtekst vil på listen fremgå med fed skrift.

13.1 Litteratur

Carsten Munk-Hansen, ”Retsvidenskabsteori”, 3. udgave, 1. oplag, Djøf forlag, 2022.
Munk-Hansen, Carsten, ”Retsvidenskabsteori”, 2022

Carsten Munk-Hansen, ”Den Juridiske Løsning”, 2. udgave, 1. oplag, Djøf forlag, 2021.
Munk-Hansen, Carsten, ”Den Juridiske Løsning”, 2021

Trine Baumbach og Thomas Elholm, “Udvalgte delikter i straffeloven – en introduktion”, 1 udgave, 1. oplag, Djøf forlag, 2021.
Baumbach, Trine mf. ”Udvalgte delikter i straffeloven – en indtroduktion”, 2021

Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn, ”Kommenteret straffelov – Speciel del”, 12. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag, 2022.
Elholm, Thomas mf. ”Kommenteret straffelov – Speciel del”, 2022

13.2 Hjemmesider

<u>Faktabaserede hjemmesider</u>

Det Kriminal Præventive Råd, **DKR, 2018, ”Cybercrime - Når kriminaliteten rykker online”,** besøgt 16-05-2023
https://dkr.dk/media/6921/cybercrimefolder2018.pdf

Det Kriminal Præventive Råd, **DKR, 16-11-2022, ”IT-kriminalitet i tal”**, besøgt 16-05-2023
https://dkr.dk/it/it-kriminalitet-i-tal

Center for cybersikkerhed, ”Cybertruslen”, besøgt 16-05-2023
https://www.cfcs.dk/da/cybertruslen/

BlueVoyant, 2022,**”Cybercrime: History, Global Impact & Protective Measures”,** besøgt 16-05-2023
https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022

Wikipedia, 2019, ”Phone-Phreaking”, besøgt 16-05-2023 (Sidst ændret 6. januar 2019 kl. 00:55)
https://da.wikipedia.org/wiki/Phone-phreaking

Wikipedia, 2023, ”KGB”, besøgt 16-05-2023 (Sidst ændret 18. april 2023 kl. 01:18.)
https://da.wikipedia.org/wiki/KGB

E-lov, juridisk ordbog, 05-10-2014, "forsæt", besøgt 16-05-2023
https://www.elov.dk/juridisk-ordbog/forsaet/

Artikler

Charlotte Hansen, TV2, 11-05-2023, ""Mathias fra banken" franarrede…", besøgt 16-05-2023
https://nyheder.tv2.dk/lokalt/2023-05-11-mathias-fra-banken-franarrede-aeldre-damer-tusindvis-af-kroner?fbclid=IwAR3iTYzAuQcjX3dZDqSgR5Tb4TbyPENVivtuzKxuszNh4ZduhIVjZSAs5ac

Digitaliseringsstyrelsen, 02-2021, "Digitaliseringsstyrelsen: Danmarks Radios historier om identitetstyveri og misbrug af NemID er misvisende og skaber utryghed på fejlagtigt grundlag", besøgt 16-05-2023
https://digst.dk/nyheder/nyhedsarkiv/2021/februar/danmarks-radios-historier-om-identitetstyveri-og-misbrug-af-nemid-er-misvisende-og-skaber-utryghed-paa-fejlagtigt-grundlag/

Camilla Bøgeholt Lund, TV2 Fyn, 23-01-2017, "Kriminelle vil hellere sidde hjemme i sofaen: Databedrageri er eksploderet", besøgt 16-05-2023.
https://www.tv2fyn.dk/datakriminalitet-pa-fyn/kriminelle-vil-hellere-sidde-hjemme-i-sofaen-databedrageri-er-eksploderet

Katie Chadd, Cybercrime Magazine, 30-11-2020, "The History Of Cybercrime And Cybersecurity, 1940-2020", besøgt 16-05-2023
https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020

Astrid Søndberg mf., TV2, 07-04-2016, "Trods mørketal: 100 nye sager om it-svindel - hver dag", besøgt 16-05-2023
https://nyheder.tv2.dk/krimi/2016-04-07-trods-moerketal-100-nye-sager-om-it-svindel-hver-dag

Julie Schneider, Berlingske, 08-07-2021, "Truslen fra cyberkriminalitet stiger: »Det her handler om hele livsnerven i vores samfund«", besøgt 16-05-2023 https://www.berlingske.dk/virksomheder/truslen-fra-cyberkriminalitet-stiger-det-her-handler-om-hele

Europa-Parlamentet, 23-11-2022, **"Hvorfor er cybersikkerhed vigtigt, og hvad koster cyberangreb EU?"**, besøgt 16-05-2023
https://www.europarl.europa.eu/news/da/headlines/society/20211008STO14521/hvorfor-er-cybersikkerhed-vigtigt-og-hvad-koster-cyberangreb-eu

Europa-Parlamentet, 23-11-2022, **"A cybersecure digital transformation in a complex threat environment"**, besøgt 16-05-2023
https://digital-strategy.ec.europa.eu/en/library/cybersecure-digital-transformation-complex-threat-environment-brochure

Center for cybersikkerhed, 03-04-2020, " Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien", besøgt 16-05-2023
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/covid-19/

Kromann Reumert, 06-04-2020, ”COVID-19: Folketinget indfører hjemmel for firedobbelte bøder og fængsel i op til 20 år for "hjælpepakkesvig"”, besøgt 16-05-2023
https://kromannreumert.com/nyheder/covid-19-folketinget-indfoerer-hjemmel-firedobbelte-boeder-faengsel-op-til-20-aar

DKR, Via Ritzau, 21-04-2022, ”Over 150.000 danskere er ofre for it kriminalitet”, besøgt 16-05-2023
https://via.ritzau.dk/pressemeddelelse/over-150000-danskere-er-ofre-for-it-kriminalitet?publisherId=9329615&releaseId=13648285
Freja Thorbech, Finansforbundet, 08-05-2023, ”Banker fik stoppet svindel for 113 millioner kroner”, besøgt 16-05-2023
https://finansforbundet.dk/dk/nyheder/2023/banker-fik-stoppet-svindel-for-113-millioner-kroner/?fbclid=IwAR1XuGdalZrXEqRShwvgFGar8AlD65kKkuTMl2zoLCXZ1QpYbfMDRf-H_hc

Andrew Douthwaite, Virtualarmour, 26-10-2022,” Cybercrime’s Evolution Since the 80’s: Historical Facts and Figures”, besøgt 16-05-2023
https://virtualarmour.com/cybercrimes-evolution-since-the-80s

Statistik

Danmarks statistik, 02-02-2023, ”Fortsat stigning i anmeldelser om bedrageri”, besøgt 16-05-2023
https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=40257

13.4 Betænkninger

Betænkning nr. 1417, Delbetænkning VIII, Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet, 2002, ”IT-Kriminalitet”, besøgt 16-05-2023
https://www.xn--betnkninger-c9a.dk/wp-content/uploads/2021/08/1417.pdf

Betænkning nr. 1032, Straffelovrådet, 1985, ”datakriminalitet”, besøgt 16-05-2023
https://www.elov.dk/media/betaenkninger/Straffelovraadets_betaenkning_om_datakriminalitet.pdf

13.5 Retspraksis

U 1937.376 V
U.1940.1113 Ø
JD 1940.130 U
U 1942.419 Ø
U 1956.131 V
U.1970.838 V
U 1974.243 Ø
U 1975.434 V
U 1978.572 V
U 1980.628 V
U 1982.1187/1 V
U 1987.216 Ø
U 1992.65/1 Ø
U 1993.667 H:
U 1994.97 V
U 2000.1893 Ø
U 2001.2110 V
TfK 2003.784 Ø

TfK 2004.539 Ø

TfK 2006.603 V

TfK 2008.647 Ø

U 2008.1607 H (U 2007.1444 Ø)

TfK 2009.48 Ø

TfK 2010 343/2 Ø

TFK 2010.785 V

TFK 2011.396/2 Ø

TfK 2011.737 V

TfK 2014.577 V

TfK 2014.1035 V

U 2014.1688 V

U 2014.2941 V

TfK 2016.779 Ø

TfK 2016.1218 V

TfK 2017.9 V

TfK 2017.1158/2 Ø

TfK 2020.459 V

TfK 2021.1115 Ø

TfK 2022.173 Ø

TfK 2022.203 V

13.6 Lovgivning

Lovbekendtgørelse 2022-09-28 nr. 1360 – Straffeloven

German Criminal Code - (Strafgesetzbuch – StGB), besøgt 17-05-2023
https://www.gesetze-im-internet.de/englisch_stgb/