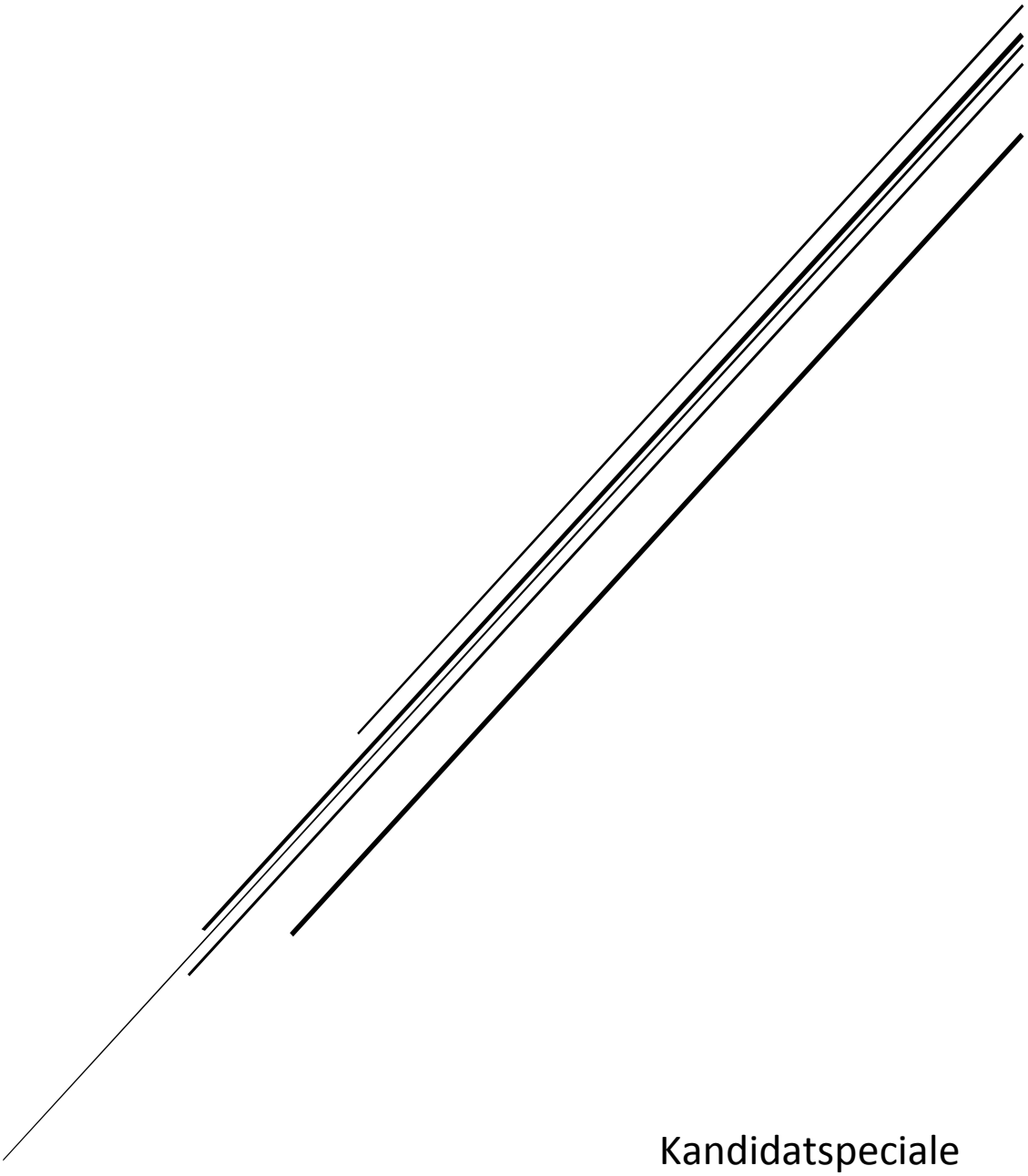
DATAHÆRVÆRK

En analyse af den strafferetlige beskyttelse af data



Kandidatspeciale
Aalborg Universitet

Titelblad

Titel: Datahærværk

Title: Data vandalism

Uddannelse: Jura, Aalborg Universitet

Projekt: Kandidatspeciale

Fagområde: Strafferet

Omfang: 59 sider

Forfatter: Rune Christen Lauridsen (studienummer: 20137084)

Vejleder: Birgit Feldtmann

Afleveringsdato: 17. maj 2018

Indholdsfortegnelse

Kapitel 1
Introduktion

1.1 Indledning

Dagens Danmark er kendetegnet som et informationssamfund, i modsætning til det tidligere industrisamfund. Data i form af information, spiller derfor i dag en vigtig rolle, og fremstår som et værdifuldt gode for både private mennesker og virksomheder. Fordi data i dag er et så centralt element i vores samfund, er beskyttelsen af data derfor også vigtigt. Ikke mindst, er den strafferetlige beskyttelse af data afgørende for, at der kan opstilles et effektivt værn mod datahærværk.

Straffelovens[1] § 291, stk. 1, har i dag følgende ordlyd:

"Den, der ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, straffes med bøde eller fængsel indtil 1 år og 6 måneder."

Spørgsmålet er her, hvordan data er beskyttet mod hærværk, og om denne beskyttelse er fyldestgørende, set i sammenhæng med ny teknologi.

Til illustration af problematikken vil følgende eksempel blive fremført:

Peter har en google-konto, hvor han har gemt og opbevaret data, f.eks. i form af dokumenter. Peter er vældig glad for denne service, da han nu kan tilgå sine data lige meget, hvor han er henne i verden og uafhængigt af, hvilken enhed han anvender. Dataene er således svævende i skyen. En dag opstår der en tvist mellem Peter og Google. Denne tvist ender desværre ud i, at Peters data bliver slettet.

Spørgsmålet er nu, hvordan denne problematik skal løses. Hvis data fortolkes i overensstemmelse med ordet "ting" i straffelovens § 291, stk. 1, er problemstillingen hurtigt løst. Det ses dog i retspraksis, at data formentlig ikke har en selvstændig beskyttelse mod hærværk. I stedet er beskyttelsen af data afledet, da det er det databærende medie, som er beskyttet. Den afledte beskyttelse af data vil i ovenstående eksempel skabe problemer. Er der tale om ødelæggelse mv.

[1] LBK nr. 977 af 09/08/2017 – herefter benævnt "straffeloven"

af en andens ting, når det er serveren, som anses for at være omfattet af hærværksbestemmelsen, i modsætning til dataene selv? Hvem er ofret i sagen, når det er det databærende medie, som anses for ødelagt, i medfør af straffelovens § 291, stk. 1. Hvis det er Google (som er ejeren af serveren) har Peter således ikke mulighed for at bede politiet om at påtale forholdet, jf. straffelovens § 305, stk. 1.

Ovenstående problemstilling har derfor ledt til nedstående problemformulering:

1.2 Problemformulering

Hvordan er data strafferetligt beskyttet mod hærværk, jf. straffelovens § 291, stk. 1?

Er den strafferetlige beskyttelse af data fyldestgørende, særligt i relation til udviklingen af ny teknologi?

1.3 Afgrænsning

Centralt for denne afhandling er hærværk af data og fortolkningen af ordet ”ting” i straffelovens § 291, stk. 1. Hærværk af grov beskaffenhed er angivet i straffelovens § 291, stk. 2. I afhandlingen vil der være en kort gennemgang af, hvornår der er tale om hærværk af grov beskaffenhed. Dette sker, fordi der i nogle af de domme, som er nævnt i afhandlingen, henvises til straffelovens § 291, stk. 2. Tilregnelsesformerne i straffelovens § 291 er forsæt og i visse tilfælde grov uagtsomhed. Tilregnelsesformerne vil kort blive nævnt, men herudover er fokus på de objektive krav til bestemmelsen. I straffelovens § 291, stk. 4 er der angivet en regel om strafskærpelse, som ikke vil blive behandlet yderligere i denne afhandling.

Der i denne afhandling henvist til andre bestemmelser i straffeloven end § 291, herunder §§ 276 og 293. Dette er sket som et led i fortolkningen af ordet ”ting” i straffelovens § 291. Ordet ”ting”, er således afgrænset op imod andre bestemmelser i straffeloven, hvor ordet ”ting” også fremgår. Formålet med denne afgrænsning er dog ikke at foretage en selvstændig analyse af de pågældende bestemmelser.

Herudover er §§ 171 og 263 også inddraget. Dette er sket for at belyse en tendens fra lovgivers side til at foretage ændringer i straffeloven, når den teknologiske udvikling har krævet det. Ligeledes vil disse bestemmelser heller ikke være genstand for en selvstændig analyse.

Der er i denne afhandling perspektiveret til norsk ret. Dette er sket for at vise, hvordan man i Norge har anvist en løsning til problemstillingen angående hærværk af data. Meningen har dog ikke været at foretage en nærmere analyse af den norske hærværksbestemmelse.

1.4 Metode

Denne afhandling har haft til formål at afklare, hvordan data er beskyttet mod hærværk, og om denne beskyttelse er fyldestgørende set i sammenhæng med udviklingen af ny teknologi. For at belyse dette er der i afhandlingen gjort brug af den retsdogmatiske metode. Via den retsdogmatiske metode analyseres og beskrives den gældende retstilstand.[2] For at fastlægge gældende ret anvendes relevante retskilder, herunder loven, forarbejder til loven og retspraksis. Herudover anvendes også forskellig juridisk litteratur, som fungerer som et fortolkningsbidrag. Ved at fortolke og analysere retskilderne klarlægges gældende ret på området for hærværk af data.

1.5 Afhandlingens opbygning

I kapitel 2 er der redegjort for henholdsvis legalitetsprincippet og fortolkningsprincipperne. I kapitel 3 vil data blive defineret ud fra Cybercrime-konventionen. Yderligere vil der her også blive redegjort for den tekniske forståelse af data. Der er til sidst i kapitel 3 givet er kort overblik over dele af datakriminaliteten for at fastslå, hvilke bestemmelser der beskytter henholdsvis systemet, og hvilke der beskyttet data. I kapitel 4 analyseres retspraksis og relevante betænkninger for at klarlægge, hvordan data i dag er beskyttet mod hærværk. Til sidst i kapitel 5 er det undersøgt, om data kan fortolkes i overensstemmelse med ordet ”ting” i straffelovens § 291, stk. 1. Efter konklusionen, er der perspektiveret til norsk ret for at fastlægge, hvordan man i Norge har behandlet problemstillingen omkring hærværk af data.

[2] Carsten Munk-Hansen, Retsvidenskabsteori, side 190

Kapitel 2
Det strafferetlige hjemmelskrav og fortolkning

I dette kapitel vil det strafferetlige legalitetsprincip blive gennemgået, ligesom fortolkningsprincipperne ved lovfortolkning vil blive gennemgået. Dette sker for at belyse de fundamentale elementer, som er relevante for denne afhandling.

2.1 Legalitetsprincippet

Det strafferetlige legalitetsprincip tager udgangspunkt i straffelovens § 1. Legalitetsprincippet medfører, at straf skal have hjemmel i lov. Dette betyder, at et faktisk begået forhold skal være en overtrædelse af en materiel lovbestemmelse, som kan medføre straf, eller også skal et faktisk begået forhold kunne sidestilles med et forhold, som loven sanktionerer med straf. I begge tilfælde udgør forholdet en forbrydelse. Betydningen af at et forhold kun kan straffes, hvis det er kriminaliseret ifølge lov, er at selvom et givent forhold er strafværdigt på domstidspunktet, kan der ikke ske domfældelse, hvis forholdet endnu ikke er kriminaliseret. Ligeledes vil forsøg i denne sammenhæng ikke kunne straffes, da forsøgsstraf stadig forudsætter, at den tilsigtede handling er kriminaliseret ved lov.[3]

Når lovgiver skal formulere, hvad der skal kunne medføre straf, gælder det om at ramme en formulering, som ikke bliver af kasuistisk karakter, som f.eks. var tilfældet med en del af bestemmelserne i Danske Lov. Herved opstod der tilfælde, hvor strafværdige handlinger ikke var kriminaliseret, og hvor domstolene indimellem valgte at pålægge straf uden egentlig tilstedeværelse af lovhjemmel.[4] Omvendt er det vigtigt, at bestemmelserne i straffeloven ikke bliver så bredt formuleret, at enhver borger ikke kan forudsige sin retsstilling, og derved i et vist omfang fratages muligheden for at skaffe sig viden om, hvad der er gjort strafbart.

[3] Trine Baumbach, Det strafferetlige legalitetsprincip, side 152 ff.
[4] Waaben, Ansvarslæren, side 70

Det er behandlet i litteraturen, om der gælder et klarhedskrav i relation til straffelovens § 1. Klarhed i lovgrundlaget henføres normalt til en given lovbestemmelses ordlyd. En lovbestemmelse kan være uklar, når lovbestemmelsens indhold kun giver et usikkert grundlag for, hvilke handlinger, som i det hele taget må siges at være omfattet af lovbestemmelsen.[5]

Som et eksempel kan fremhæves færdselslovens[6] § 3, stk. 1:

> *"Trafikanter skal optræde hensynsfuldt og udvise agtpågivenhed, så at der ikke opstår fare eller forvoldes skade eller ulempe for andre, og således at færdslen ikke unødigt hindres eller forstyrres. Der skal også vises hensyn over for dem, der bor eller opholder sig ved vejen."*

Et andet tilfælde af uklarhed kan også forekomme, hvor en bestemmelses ordlyd egentlig dækker handlinger af en given art, men hvor udstrækningen af ordlyden må siges at være usikker.[7] Netop udstrækningen af ordet "ting", i henhold til straffelovens § 291, stk. 1, er i denne afhandling helt central for at belyse, på hvilken måde data er beskyttet mod hærværk, og om denne beskyttelse overhovedet er fyldestgørende, særligt med henblik på, hvordan teknologien har udviklet sig.

Trine Baumbach anfører at hensynet til borgernes retssikkerhed og straffelovgivningens demokratiske legalitet medfører, at lovgiver skal bestræbe sig på at være så præcise som muligt ved udformningen af straffebestemmelserne. Hun mener dog ikke dette betyder, at der i straffelovens § 1 kan opstilles et såkaldt klarhedskrav. Dette forklares ud fra, at der efter straffelovens § 1 kan sluttes lovanalogt samtidig med, at det må forudsættes, at der ud for enhver lovbestemmelse må kunne ske en fortolkning før lovbestemmelsen kan anvendes i praksis. Det vil således ikke altid være muligt at udforme en lovbestemmelse, som i alle henseender, og på én og samme tid, kan være fuldstændig dækkende i dens ordlyd. Kan en lovbestemmelse derfor anses for at være uklar er den ikke i samme ombæring ugyldig og skal formentlig heller ikke tilsidesættes af domstolene. Giver en bestemmelse ingen vejledning ift. dens normative indhold kan resultatet heraf blive en frifindelse, ikke på baggrund af at lovbestemmelsen ikke er i overensstemmelse med

[5] Trine Baumbach, Det strafferetlige legalitetsprincip, side 157-159
[6] LBK nr. 38 af 05/01/2017 (færdselsloven)
[7] Trine Baumbach, Det strafferetlige legalitetsprincip, side 159

klarhedskravet, men fordi der ikke er hjemmel til at dømme. Om der hjemmel til at dømme afgøres dermed ud fra ordlyden og i sidste ende ud fra en fortolkning af ordlyden.[8]

Ud over straffelovens § 1 har Danmark også forpligtet sig til at overholde EMRK[9]. I EMRK er legalitetsprincippet også fastslået, jf. EMRK artikel 7. Dette betyder at EMRK også forudsætter lovhjemmel før der kan idømmes straf.

2.2 Fortolkning

I juraens verden anvendes lovfortolkning, når en lovbestemmelses indhold skal fastlægges. Som tidligere beskrevet kan en lovbestemmelse fremstå uklar, når der tvivl om ordlydens udstrækning.

I relation til strafferetten er lovfortolkning særlig vigtig i forhold til at afgøre, om en bestemt handling er strafbar, eller i modsat retning skal lede til en frifindelse. Den strafferetlige lovfortolkning følger som udgangspunkt de almindelige regler for lovfortolkning, dog gælder der for strafferetten også særegne fortolkningsprincipper.[10]

Den almindelige lovfortolkning rummer først og fremmest den præciserende, indskrænkende og udvidende fortolkning. Via den præciserende fortolkning fastslås det ud fra ordlyden, hvilken forståelsesmåde, der er den rigtige. Denne fortolkning tager afsæt i, at der findes flere forskellige naturlige forståelsesmåder, hvorpå ordlyden kan fortolkes. Den præciserende fortolkning vil altid holde sig inden for ordlydens naturlige grænse og vil dermed hverken udvide eller indskrænke anvendelsesområdet. Den præciserende fortolkning giver således alene en klarere forståelse af ordlyden end udsagnet i ordlyden i sig selv giver.[11] Ved en indskrænkende fortolkning, holdes elementer, der er dækket af ordlyden, uden for anvendelsesområdet. Ved en udvidende fortolkning findes den endelige fortolkning af bestemmelsen at ligge uden for den naturlige sproglige forståelse af ordlyden. Den udvidende fortolkning er en fortolkningsvariant, som bevæger sig uden for ordlyden, hvorved bestemmelsen udvides.[12] I sammenhæng med den udvidende fortolkning findes analogien. Trine Baumbach anfører, at grænsen mellem en udvidende fortolkning og analogi er hårfin, og at der således ikke er en egentlig forskel på en

[8] Trine Baumbach, Det strafferetlige legalitetsprincip, side 166-167
[9] LBK nr. 750 af 19/10/1998
[10] Trine Baumbach, Det strafferetlige legalitetsprincip, side 259-261
[11] Trine Baumbach, Det strafferetlige legalitetsprincip, side 265
[12] Trine Baumbach, Det strafferetlige legalitetsprincip, side 267

udvidende fortolkning og analogi.[13] Analogien bruges når en lovbestemmelse anvendes på et forhold, som ikke er omfattet af loven. Ikke enhver analogi har hjemmel i straffelovens § 1. Der skal således være tale om en fuldstændig lovanalogi. Hermed skal der som det første være tale om en anvendelse af en eksplicit lovbestemmelse. Dernæst skal denne lovbestemmelse have en sådan lighed med det af lovbestemmelsens omfattede forhold. Ligheden skal være så stor, at det må karakteriseres som ren formalisme, at det pågældende forhold ikke er kriminaliseret.[14]

Som eksempel på en sag, hvor en analogi blev afvist, er Østre Landsrets dom af 13. februar 1995. Her udtalte Østre Landsret, at urigtige erklæringer afgivet på diskette, ikke var omfattet af straffelovens dagældende § 163, eller dennes analogi, omhandlende afgivelse af skriftlige urigtige erklæringer.[15] Retten henviste til forarbejderne fra 1985, hvor det er anført at straffelovens § 163 kun omfatter skriftlige erklæringer, og at bestemmelsen dermed ikke er brugbar i tilfælde, hvor der anvendes "datateknik".[16]

I andre sager har domstolene været villige til at fortolke udvidende. Dette er kommet til udtryk ved dommen U 1940.156 Ø hvor Østre Landsret dømte efter en analogi af den ældre § 263 i straffeloven, som i 1940 kun omhandlede retsstridige brevåbninger. I sagen var der tale om en hemmelig aflytning, hvor der blev anvendt lytteudstyr.[17]

Slutresultatet blev også en udvidende fortolkning i dommen U 1996.356 Ø. Her var T tiltalt for overtrædelse af den dagældende § 2 i indsamlingsloven. Denne bestemmelse forbød indsamlinger ved anvendelse af pyramidespil. Systemet var opbygget på samme måde som et traditionelt pyramidespil, men med brug af disketter. Normalt er et pyramidespil opbygget via en personlig skriftlig henvendelse, som viderebringer en opfordring til at betale et vist beløb. Af denne grund valgte byretten af frifinde. Landsretten valgte dog at anse T for skyldig, da systemet er lavet på samme måde, som det traditionelt ses med kædebreve, og da formålet var at opnå en uberettiget vinding. Landsretten tillagde det således ikke vægt, at kommunikation var sket via disketter, da

[13] Trine Baumbach, Det strafferetlige legalitetsprincip, side 395 ff.
[14] Ibid.
[15] Dommen er refereret fra, Mads Bryde Andersen, IT-retten, side 725
[16] Betænkning nr. 1032 (1985), side 64
[17] Dommen er refereret fra, Mads Bryde Andersen, IT-retten, side 724

fremgangsmåden kunne anses som værende i overensstemmelse med fremgangsmåden ved afsendelse af kædebreve.

På baggrund af ovennævnte domme er det ikke let at forudsige, hvordan domstolene vil se på sager, hvor straffebestemmelser skal fortolkes udvidende. Retspraksis på området omhandlende den fuldstændige lovanalogi er ikke mangfoldig. Dette kan begrundes ud fra, at domstolene helst dømmer ud fra en præciserende ordlydsfortolkning eller helt frifinder.[18]

Den almindelige fortolkningslærer indeholder yderligere, subjektiv, objektiv og teleologisk fortolkning. Subjektiv fortolkning tager sit udgangspunkt i, hvad der kan kaldes lovgivers vilje. Med denne fortolkningsmetode forsøges det at klarlægge, hvilke handlinger lovgiver har villet ramme med lovreguleringen. Dette sker via forarbejder, særligt lovkommentarer eller betænkninger. Den objektive fortolkning tager sit udgangspunkt i ordlyden eller undlader at indhente fortolkningsbidrag fra forarbejderne. Teleologisk fortolkning anvender formålet med loven som fortolkningskilde. Hvis formålet med en lovbestemmelse peger i retning af en kriminalisering, selvom en handling ikke kan siges at være omfattet af ordlyden i bestemmelsen, kan formålet indgå som fortolkningsfaktor ved afgørelsen af, om der skal benyttes en fuldstændig lovanalogi. [19]

Den strafferetlige fortolkning tager, som al anden fortolkning, sit udgangspunkt i ordlyden. Der er flere forskellige strafferetlige fortolkningsvarianter, og kongruensfortolkning er en af dem. Kongruensfortolkning er en fortolkningsmåde, som fortolker et udtryk eller begreb i overensstemmelse, med hvordan udtrykket eller begrebet er blevet brugt i samme lov eller i lovgivningen generelt.[20]

2.3 Delkonklusion

Som det er redegjort for i dette kapitel, udgør legalitetsprincippet et vigtigt element inden for strafferetten. Legalitetsprincippet medfører, at straf skal have hjemmel i lov. Det er tilladeligt at anvende en analogi, men denne analogi skal være en fuldstændig lovanalogi. Der kan ikke udledes et selvstændigt krav om klarhed i medfør af legalitetsprincippet. Alle lovbestemmelser kan dog være uklare, men dette skal løses via fortolkning og ikke via en tilsidesættelse af bestemmelsen

[18] Vagn Greve mfl., Kommenteret straffelov almindelig del, side 130
[19] Trine Baumbach, Det strafferetlige legalitetsprincip, side 271-273
[20] Trine Baumbach, Det strafferetlige legalitetsprincip, side 283ff.

som værende ugyldig. Nogle bestemmelser i straffeloven er formuleret på en måde, hvor der er anvendt ord, som kan fortolkes bredt. Et eksempel på dette kan være straffelovens § 291, stk. 1, hvor udstrækningen af ordet ”ting” er relevant. I sådanne tilfælde må der ske en fortolkning af bestemmelsen for at afgrænse bestemmelsens anvendelsesområde. Udgangspunktet for al lovfortolkning er ordlyden, og denne fortolkes via en objektiv eller subjektiv fortolkning, som kan være indskrænkende, præciserende eller udvidende.

Kapitel 3
Den retlige og tekniske forståelse af data

I dette kapitel vil det blive undersøgt, hvad data er. For at kunne analysere, hvordan data er beskyttet mod hærværk, er det således nødvendigt at have en fundamental viden, om hvordan data defineres. Således vil Cybercrime-konventionens[21] relevante definitioner af data og edb-anlæg blive belyst, og herunder også Cybercrime-konventionens foranstaltninger for beskyttelse af data. Herefter vil der blive redegjort for den mere tekniske forståelse af data for at belyse, hvad ordet indeholder. Herefter vil faserne for den mere generelle IT-kriminalitet blive gennemgået. Dette sker for at belyse, i hvilken fase af it-kriminaliteten hærværk forekommer. Det er i ældre retspraksis fastlagt, at data ikke er selvstændigt beskyttet mod hærværk, men at det derimod er det databærende medie, som anses for beskyttet. Derfor vil det også blive undersøgt, hvilke bestemmelser i straffeloven, som beskytter data mod it-kriminalitet, og hvilke der beskytter edb-systemet.

3.1 Cybercrime-konventionen

Cybercrime-konventionen er vedtaget af Europarådet og har til formål, via et internationalt samarbejde, at bekæmpe it-relateret kriminalitet.[22] Dette mål skal sikres ved at de deltagende lande skal sørge for at gøre it-kriminalitet, såsom indgreb i data og indgreb i systemer, strafbart.

Konventionen blev indgået d. 23. november 2001 og trådte i kraft den 21. juni 2005. Danmark valgte at tiltræde konventionen den 1. oktober 2005[23], på baggrund af lov nr. 352 af 19. maj 2004.

[21] Europarådets konvention om IT-kriminalitet af 23. november 2001 – herefter benævnt Cybercrime-konventionen
[22] Cybercrime-konventionens præambel
[23] BKI nr. 12 af 15/03/2007

I konventionens artikel 1 er der givet definitioner på henholdsvis et ”edb-system” og ”elektroniske data”. Et ”edb-system” er ifølge konventionens artikel 1, litra a defineret som:

> *”enhver anordning eller gruppe af indbyrdes forbundne eller sammenhængende anordninger, hvoraf en eller flere udfører automatisk databehandling i henhold til et program”.*

Elektroniske data er i konventionens artikel 1, litra b defineret som:

> *”enhver gengivelse af fakta, informationer eller begreber i en form, der er egnet til behandling i et edb-system, herunder et program, der er egnet til at få et edb-system til at udføre en funktion”.*

Definitionen af data i konventionens artikel 4 vil i dette speciale blive lagt til grund for behandlingen af emnet datahærværk. Disse definitioner er fremhævet her for at lede hen til det næste aspekt i Cybercrime-konventionen, nemlig den særegne beskyttelse af edb-systemer og data.

Man har i Cybercrime-konventionen valgt at beskytte indgreb i edb-systemer i artikel 5 og indgreb i data i artikel 4. Beskyttelsen af indgreb i edb-systemer i artikel 5 er defineret som:

> *”Enhver part skal vedtage sådanne lovgivningsmæssige og andre foranstaltninger, der måtte være nødvendige for at fastsætte, at det er en strafbar handling i henhold til national ret forsætligt og uberettiget at forhindre et edb-systems funktion i alvorlig grad ved at indlæse, overføre, beskadige, slette, forringe, ændre eller undertrykke elektroniske data”*.

Indgreb i data er i artikel 4 defineret som:

> *” Enhver part skal vedtage sådanne lovgivningsmæssige og andre foranstaltninger, der måtte være nødvendige for at fastsætte, at det er en strafbar handling i henhold til national ret forsætligt og uberettiget at beskadige, slette, forringe, ændre eller undertrykke elektroniske data.”*

Disse definitioner er medtaget i dette speciale for at tydeliggøre, at data nyder sin egen særegne beskyttelse i medfør af konventionen. I tilfælde af hærværk er data dermed ikke afhængig af en

såkaldt afledt beskyttelse af edb-systemet. Med andre ord medgiver Cybercrime-konventionen en selvstændig beskyttelse af henholdsvis data og edb-systemet. Denne sondring er vigtig i sammenhæng med forståelsen af, hvordan data er beskyttet mod hærværk.

Danmark har også via lov nr. 352 af 19. maj 2004 deltaget i rammeafgørelsen om angreb på informationssystemer.[24] Denne rammeafgørelse har på samme måde som Cybercrime-konventionen til hensigt at få medlemslandene til at ulovligøre uretmæssigt indgreb i data og edb-systemer.

3.2 Data

De ovennævnte definitioner er fastlagt ud fra Cybercrime-konventionen. Cybercrime-konventionens definition af data giver dog kun en overordnet beskrivelse af data, og hvad ordet egentlig indeholder. Data kan formuleres, som en manifestation af en mening, men som ikke i sin form tilkendegiver denne mening. Data udgøres således af en mængde tegn, som først efter en bearbejdelse kan forstås som information. En forkortelse der rummer en bestemt ordsammensætning, som iagttageren ikke kender, kan umiddelbart karakteriseres som data. Giver ordsammensætningen senere mening for iagttageren, kan denne ordsammensætning karakteriseres som information. Der foregår således en proces, hvor data omdannes til information, som kan give mening for iagttageren.[25] Et konkret eksempel på, hvad data kan være, er en talkombination. Således kan talkombinationen 120595 isoleret set anses for at være en given datamængde. Denne datamængde kan omsættes til en fødselsdato, 12. maj, 1995. Talkombinationen, som før forelå som en datamængde, kan altså nu opfattes som en mængde information. Der findes forskellige datatyper, herunder heltal, flydende tal og tegn. En persons hårfarve kan således repræsenteres af et tal, f.eks. hvor 1, betyder blå.[26] I bund og grund kan der således sættes lighedstegn mellem data og information, dog således at data først bliver til information ved en form for præsentation, hvor data omsættes til information ved brug af vores sprog eller gennem andre fortolkningsmekanismer.

[24] Rammeafgørelse 2005/222/RIA
[25] Mads Bryde Andersen, IT-retten, side 108
[26] http://denstoredanske.dk/It,_teknik_og_naturvidenskab/Informatik/Software,_programmering,_internet_og_webkommunikation/data

De forskellige datatyper kan lagres både på helt almindeligt papir i den analoge verden, ligesom data kan lagres digitalt. I dette speciale er det dog kun den digitalt lagrede data, som er egnet til behandling i et edb-system, som er målet for behandlingen af emnet datahærværk.

3.3 Datakriminalitet

Flere forskellige bestemmelser i straffeloven beskytter data og edb-systemer mod ulovlig angreb, adgang og anvendelse. Denne form for kriminalitet kan betegnes på flere måder, men fælles for dem alle er, at der sker et angreb, adgang eller anvendelse på enten data selv, eller på edb-systemet. Data og edb-systemer er generelt udsat for kriminalitet på flere stadier. For at klargøre på hvilket stadie, der er tale om hærværk, redegøres der for de forskellige stadier af it-kriminaliteten. Ligeledes undersøges det om bestemmelserne beskytter data eller edb-systemet.

3.3.1 Angreb

Datakriminalitet, som udføres via et angreb, betegnes normalt som malware eller et DoS-angreb. Malware har til hensigt at ødelægge programmer, filer eller at reformattere hele harddisken. Malwaren behøver dog ikke at have til formål at ødelægge noget. Der kan også være tale om at frembringe en besked eller video for modtageren. Malwaren behøver således ikke at bestå i at ødelægge eller forvanske noget. I dette tilfælde vil malwaren dog stadig udgøre et problem, da malwaren bruger en del af computerens hukommelse. Dette kan medføre en uregelmæssighed i computerens drift og i sidste ende medføre systemnedbrud. Malware betegnes normalt som en vifte af flere forskellige ondsindede programmer, som f.eks. virus, orme, trojanske heste og keyloggere. Dette program kan aktivere sig selv over for den angrebne computer, f.eks. ved udnyttelse af sikkerhedsbrister i operativsystemer eller browseren. Programmet kan dog også være udviklet på en måde, hvor brugeren af den angrebne computer selv skal aktivere programmet. Dette kan f.eks. ske via download af programmer, som ellers fremstår uskadelige. Angrebet sker således reelt uden brugerens viden.[27]

Ransomware er en anden malwaretype, som består af en form for virus. Ransomware er kendetegnet ved, at den krypterer brugerens data. Dette medvirker til, at brugerens data ikke længere er tilgængelig for brugeren. Herefter vil de IT-kriminelle kunne fremsætte forskellige krav,

[27] Jan Trzaskowski mfl., Internetretten, side 690-691

før de vil frigive en krypteringsnøgle, som kan dekryptere brugerens data. Brugeren vil således være tvunget til at opfylde disse krav for at kunne genoprette de data, som nu er krypterede.[28]

Denial-of-service-angreb (DoS-angreb) er et angreb på brugen af edb-systemer. Angrebet sker ved at overbelaste en eller flere servere, således at de i en vis periode er uanvendelige for ejeren. En server kan overbelastes ved at sende så mange forespørgsler, at serveren ikke kan sende eller modtage andre former for information. Disse forespørgsler har normalt falske afsendere. Formålet med dette angreb er at hindre adgangen til serveren og dermed også i sidste ende slutbrugeren, som sidder og surfer rundt på en internetside.[29]

Straffelovens §§ 193, stk. 1, 291, stk. 1 og 293, stk. 2 er den strafferetlige beskyttelse mod malware, ransomware og DoS-angreb.

Hvis der er tale om "omfattende forstyrrelse" vil informationssystemer være beskyttet efter straffelovens § 193, stk. 1. Informationssystemer er en nyere betegnelse for edb-systemer. Informationssystemer kan betegnes som en computer eller et databehandlingsanlæg.[30] Der er altså her tale om en beskyttelse af edb-systemet.

Straffelovens § 291, stk. 1, beskytter "ting" mod ødelæggelse, beskadigelse og bortskaffelse. Det kan af ældre retspraksis udledes, at det er det databærende medie, som data er lagret på, som er beskyttet.[31] Men om data også er selvstændigt beskyttet mod hærværk, er emnet for dette speciale.

Straffelovens § 293, stk. 2, omhandler *"Den, der uberettiget hindrer en anden i helt eller delvist at råde over en ting"*. Ifølge forarbejderne til straffelovens § 293, stk. 2, omfatter bestemmelsen både fysiske og elektroniske rådighedshindringer.[32]

3.3.2 Adgang

Straffelovens § 263, stk. 2 beskytter adgangen til oplysninger og programmer, som er bestemt til at bruges i et informationssystem. Bestemmelsen kan også betegnes som hacking-bestemmelsen.

[28] Ibid
[29] Jan Trzaskowski mfl., Internetretten, side 696-698
[30] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 322.
[31] U 1987.216 Ø (Fagforeningssagen)
[32] Lovkommentaren til lov nr. 352 af 19/05/2004, afsnit 5.2.1

Hacking er kendetegnet ved at en hacker, via et informationssystem, forsøger at skaffe sig uberettiget adgang til oplysninger eller programmer. Hackeren forsøger således at opnå adgang til et område, som kan betragtes som værende utilgængeligt for hackeren. Fredskrænkelsen består således i at skaffe sig adgang til et område, som er beskyttet af privatlivets fred.

Straffelovens § 263, stk. 2, omhandler den situation, hvor en udenforstående person forsøger at koble sig på et system, enten via nettet eller via et lukket lokalt netværk. Herudover omfatter bestemmelsen også personer, som egentlig har en lovlig adgang til systemet, men som overskrider deres mandat.[33]

Det fremgår af § 263, stk. 2, at beskyttelsesinteressen er oplysninger og programmer. Det fremgår da også af straffelovsrådets betænkning af 1985, at *"(…) den pågældende skal have opnået forbindelse til dettes indhold, medens det på den anden side ikke kræves, at han bevisligt har fået kendskab til noget."*[34]

I dommen U 2000.1450 Ø, var T tiltalt for 2 forhold, hvor det ene handlede om fuldbyrdet overtrædelse af straffelovens § 263, stk. 2, og det andet, som handlede om forsøg på overtrædelse af § 263, stk. 2. T havde i det første forhold anvendt et hackerprogram, hvorefter han uberettiget skaffede sig adgang til A's oplysninger, herunder A's brugeridentitet og password. I det andet forhold blev T straffet for forsøg, da T forsøgte at skaffe sig afgang til B's computer, hvilket dog mislykkedes, da B havde installeret et antivirusprogram.

Dommen er et udtryk for at beskyttelsen, efter § 263, stk. 2, er kategoriseret til oplysningerne på computeren og ikke informationssystemet selv.

[33] Jan Trzaskowski mfl., Internetretten, side 706
[34] Betænkning 1032 (1985), side 26

3.3 Delkonklusion

I dette kapitel er det blevet undersøgt, hvordan data og edb-systemer kan defineres. Ud fra Cybercrime-konventionen er det blevet fastlagt, at data kort sagt skal anses for at være fakta, informationer, begreber eller programmer, som kan indgå i et edb-system. Et edb-system skal anses for en anordning, som udfører automatisk databehandling. Det er også blevet klarlagt, at data skal anses for værende selvstændigt beskyttet i henhold til Cybercrime-konventionens artikel 4. Hernæst er data også blevet forklaret ud fra en mere teknisk forståelse, som værende datatyper bestående af heltal, flydende tal og tegn. Slutteligt er der blevet fokuseret på den mere generelle IT-kriminalitet, for at fastslå datahærværks placering i stadierne angreb og adgang. Herudover er der også fokuseret på, om det er edb-systemet eller data, som er beskyttet af de relevante bestemmelser i straffeloven.

Kapitel 4
Afledet eller selvstændig beskyttelse af data

Dette afsnit indledes med en præsentation af straffelovens § 291. Sigtet er her navnlig at undersøge, hvilke fænomener domstolene tidligere har fortolket i overensstemmelse med ordet ”ting”. Hernæst vil den gældende retspraksis, som foreligger på området angående hærværk af data, blive analyseret. Dette sker for at belyse om data, strafferetligt, er tillagt en afledet eller selvstændig beskyttelse, og hvorvidt data kan fortolkes i overensstemmelse med ordet ”ting” i straffelovens § 291. Ved en afledt beskyttelse af data skal forstås en beskyttelse af data via det databærende medie (f.eks. en server eller computer). Ved en selvstændig beskyttelse af data forstås en beskyttelse, hvor data er direkte omfattet af straffelovens § 291, på højde med fysiske ”ting”. Dommene som indgår er, U.1987.216Ø (Fagforeningssagen) og U.2015.3615Ø (CSC-sagen). Som det ses er der nogle år imellem de to domme, og derfor er det naturligt at se på. om der er sket en udvikling fra slutningen af 1980’erne til i dag. Der er ikke en mangfoldig retspraksis på området, men den retspraksis, som foreligger er central ift. problemstillingen angående hærværk af data.

Straffelovsrådet og Brydensholt-udvalget har i betænkninger, som er udgivet i henholdsvis 1985 og 2002, diskuteret anvendelsen af bestemmelserne i straffeloven set i relation til datakriminalitet. Også anvendelsen af hærværksbestemmelsen i relation til data er overvejet. Disse overvejelser fremstår som et vigtigt element, i forståelsen af, om data er beskyttet mod hærværk og i givet fald hvordan.

Sidst i kapitlet vil udfordringerne vedrørende beskyttelsen af data, set i forhold til udviklingen af ny teknologi, blive præsenteret.

4.1 Straffelovens § 291 historisk

Der har i dansk strafferet længe været hjemmel til at straffe hærværk. Således går hærværksbestemmelsen helt tilbage til straffeloven af 1866. I straffeloven af 1866 gik hærværksbestemmelsen under § 296 og hed følgende:

> *"Ødelægger eller beskadiger Nogen ellers forsætlig fremmed Eiendom, bliver han, forsaavidt Forholdet ikke falder ind under strængere Straffebestemmelser, at straffe med Bøder eller Fængsel. Offentlig Paatale finder kun Sted, naar Handlingen har medført Forstyrrelse af den offentlige Fred eller været forbunden med Overtrædelse af Politiforskrifter."*

Det ses af bestemmelsen, at den kun omfatter ødelæggelse og beskadigelse. Bortskaffelse, som i dag er omfattet af § 291, var således ikke ulovliggjort efter bestemmelsen. Det ses også, at der ikke er angivet en egentlig strafferamme, ligesom bestemmelsen i udgangspunktet var omfattet af privat påtale. Kun når der var tale om "forstyrrelse af den offentlige orden" eller en overtrædelse af "politiforskrifter" var påtalen offentlig.

Som den sidste straffelovsbetænkning før straffeloven af 1930 udkom straffelovskommissionens betænkning af 1923. Hærværksbestemmelse fra straffeloven af 1930 lød:

> *"Stk. 1. Den som ødelægger, beskadiger eller bortskaffer Ting, der tilhører en anden, straffes med Bøde, Hæfte eller med fængsel indtil 1 Aar.*
>
> *Stk. 2. Øves der Hærværk af betydeligt Omfang, eller er Gerningsmanden tidligere fundet skyldig efter nærværende Paragraf eller efter §§ 180, 181, 183, Stk. 1 og 2, 184, Stk. 1, 193 eller 194, kan straffen stige til Fængsel i 4 Aar.*
>
> *Stk. 3. Forvoldes Skaden under de i Stk. 2 nævnte omstændigheder af grov Uagtsomhed, er straffen Bøde, Hæfte eller Fængsel indtil 6 Maaneder."*

I forhold til hærværksbestemmelsen fra 1886, som kun medtog ødelæggelse og beskadigelse, foreslog straffelovskommissionen af 1923 også en tilføjelse af bortskaffelse af "ting". Dette skete for at tydeliggøre at bestemmelsen også omfatter den situation, hvor en "ting" fjernes, og således

kun ved *"vanskelige eller bekostelige Foranstaltninger kan faas tilbage."*[35]
Straffelovskommissionen af 1923 foreslog også strafferammen på henholdsvis 1 år i stk. 1 og 4 år i stk. 2. Påtalereglen gik også fra et udgangspunkt om privatpåtale i 1866-straffeloven til et udgangspunkt om betinget offentligt påtale.[36] Herudover krævedes der ikke længere kun forsæt som den subjektive betingelse, men nu også uagtsomhed.

4.2 Straffelovens § 291 gældende

Straffelovens § 291 har i dag følgende ordlyd:

> *"Den, der ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, straffes med bøde eller fængsel indtil 1 år og 6 måneder.*
> *Stk. 2. Øves der hærværk af betydeligt omfang eller af mere systematisk eller organiseret karakter, eller er gerningsmanden tidligere fundet skyldig efter nærværende paragraf eller efter § 180, § 181, § 183, stk. 1 og 2, § 184, stk. 1, § 193 eller § 194, kan straffen stige til fængsel i 6 år.*
> *Stk. 3. Forvoldes skaden under de i stk. 2 nævnte omstændigheder af grov uagtsomhed, er straffen bøde eller fængsel indtil 6 måneder.*
> *Stk. 4. Ved fastsættelse af straffen efter stk. 1 og 2 skal det indgå som en skærpende omstændighed, at forholdet er begået, mens eller i umiddelbar forlængelse af at der i området foregår grov forstyrrelse af ro og orden på offentligt sted."* (min understregning)

Hærværksbestemmelsen har, som den ser ud i dag, ikke ændret sig meget fra bestemmelsen i 1930-straffeloven. Dog er det et gennemgående træk, at hæftestraffen som sanktion i dag er afskaffet. Det er ligeledes et gennemgående træk, at strafferammerne er forhøjet. Som noget nyt er der i den gældende bestemmelse i dag indsat en strafskærpelsesbestemmelse i stk. 4.

Straffelovens § 291 er i dag placeret i kapitel 28 omhandlende formueforbrydelser. En formueforbrydelse kan karakteriseres som en forbrydelse, der har sigte på at angribe andres formuegoder. Mange af bestemmelserne i starten af kapitel 28 kan karakteriseres som

[35] Straffelovsbetænkning 1923, mot. 383
[36] Straffelovsbetænkning 1923, mot. 384

berigelsesforbrydelser, hvor det afgørende moment er en opnåelse af en uberettiget vinding, skabt gennem et retsstridigt formuetab hos den forurettede. Straffelovens § 291 kan ikke betegnes som en berigelsesforbrydelse, da der i § 291 ikke forekommer en uberettiget vinding for gerningsmanden, men udelukkende et tab for den forurettede.[37] I straffeloven før 2001 var kapitel 28 delt op i to kapitler. Således var §§ 276-290 omfattet af kapitel 28, omhandlende berigelsesforbrydelser. §§ 291-305 var omfattet af kapitel 29, omhandlende andre strafbare formuekrænkelser.[38] Om denne opdeling er der i straffelovsbetænkningen fra 1923 anført, at kapitel 29 omfatter formuekrænkelser, hvor der ikke foreligger berigelseshensigt, men som dog er så alvorlige, at de ikke skal være omfattet af Lov om Forseelser. [39] Den nuværende samling af §§ 276-305 blev samlet i kapitel 28 for at gøre det muligt at samle de nye bestemmelser på det område, som forekommer naturligt ud fra andre formål end netop begrebet om berigelsesforbrydelser.[40]

4.2.1 Objektive og subjektive krav

4.2.2 Objektive krav

Som ved alle andre straffebestemmelser i straffeloven er der en række subjektive og objektive momenter i gerningsindholdet, som skal være opfyldt før gerningsmomentet § 291 kan anses for være realiseret.

I forhold til de objektive krav kan det først og fremmest nævnes, at der skal være tale om en "ting". I 1923 fastslog straffelovskommissionen, at ordet "ting" omfatter løsøre og fast ejendom.[41] "Ting" vil derfor omfatte fysiske genstande af forskellig art, ligesom dyr også vil være omfattet.[42]

Ud fra domspraksis er ordet "ting" blevet fortolket. Det kan nævnes at Vestre Landsret i dommen U.1975.972 V, anså en *hund* for at kunne fortolkes i overensstemmelse med tingsbegrebet. I sagen nedskød T en omstrejfende hund til en værdi af 5000 kr., og blev dømt skyldig efter straffelovens § 291, stk. 1.

[37] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 581
[38] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 582
[39] Straffelovsbetænkning 1923, mot. 382
[40] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 582
[41] Straffelovsbetænkning 1923, mot. 382
[42] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 667

I TfK.2011.668 V, blev T fundet skyldig i en overtrædelse af straffelovens § 291, stk. 2, efter at have fældet 24 *træer* som var ejet af Skov- og Naturstyrelsen. Retten fandt det bevist, at T vidste, at træerne tilhørte Skov- og Naturstyrelsen. Retten valgte at dømme efter § 291, stk. 2 (betydeligt omfang), da prisen for nye træer og beplantningen heraf anslås at koste 294.337 kr.
I U.1965.535 V, blev T fundet skyldig i at have overtrådt straffelovens § 291, stk. 1, ved at have beskadiget naboens *markvej*. Beskadigelsen skete i forbindelse med en grøftegravning.

De refererede domme viser, at domstolene er villige til at fortolke ordet "ting" forholdsvist bredt. Det skal dog understreges, at der i samtlige tre domme er tale om fysiske "ting", og altså ikke data. Det er ikke et krav, at den "ting", som der udøves hærværk mod, har en omsætningsværdi. Det har den betydning, at bortskaffelse af "ting", som må anses for at have ringe omsætningsværdi, såsom private breve og dagbøger, kan straffes efter § 291.[43]

Udover at der skal være tale om en "ting", skal denne "ting" også "tilhøre en anden". Det er angivet i straffelovsbetænkningen fra 1923, at udtrykket "tilhører en anden" er synonymt med om tingen er fremmed.[44] Ved forståelsen af om en "ting" er fremmed lægges der vægt på om tingen tilhører en anden end gerningsmanden. Uden for dette område falder således ting, som er ejerløs og ting, som gerningsmanden selv ejer.[45] I sidstnævnte tilfælde vil der formentlig kunne dømmes efter § 292, hvis en person ødelægger, beskadiger eller bortskaffer ting, hvis det sker for at unddrage dem fra at tjene sine fordringshavere.

I bestemmelsen består den strafbare handling i at ødelægge, beskadige eller bortskaffe tingen. Ved ødelæggelse forstås normalt at gøre noget ubrugelig eller værdiløs.[46] Ved beskadigelse forstås både en delvis ødelæggelse af tingen, men også andre former for beskadigelse, hvor tingen ikke som sådan bliver ødelagt.[47] Således er der afsagt flere domme angående graffitihærværk, f.eks. U.2006.21.68 Ø, hvor T blev dømt efter straffelovens § 291, stk. 2, for at have tegnet graffiti på en S-togsvogn. Det samlede erstatningskrav løb op i 24.109 kr.

[43] Jørn Vestergaard, Forbrydelser, side 205
[44] Straffelovsbetænkning 1923, mot. 383
[45] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 588
[46] http://ordnet.dk/ddo/ordbog?query=%C3%B8del%C3%A6gge
[47] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 668

Ved bortskaffelse forstås, som tidligere beskrevet, at "*Tingen skaffes af Vejen, saaledes at den ikke eller kun ved vanskelige eller bekostelige Foranstaltninger kan faas tilbage"*[48] I dommen U.1960.746/2 B*,* bortskaffede T en regnemaskine fra et kommunekontor, da han mente at han hermed udøvede en gyldig tilbageholdelsesret. Tilbageholdelsesretten var dog ikke gyldig, og retten dømte T for at bortskaffe regnemaskinen, da T havde gemt maskinen hos en person, som T ikke havde tilknytning til, og hvor det ville være svært at finde regnemaskinen.

I straffelovens § 291, stk. 2, hæves strafferammen til 6 års fængsel, hvis der er udøvet hærværk af betydeligt omfang. Der foreligger hærværk af betydeligt omfang, når ødelæggelsen mv. har et betydeligt fysisk omfang. Herudover kan der også være tale om hærværk af betydeligt omfang, når skadens størrelse medfører et tab af betydelige værdier. [49] Rigsadvokaten har i 2005 fastsat retningslinjer for strafpåstandene i sager om hærværk. Hvis værdien af skadens størrelse overstiger 15.000 kr., bør der i udgangspunktet nedlægges påstand om frihedsstraf, og forholdet bør henføres under straffelovens § 291, stk. 2. Udover beløbsstørrelsen bør der også foretages en vurdering af skærpende eller formildende omstændigheder, som f.eks. arten og antallet af hærværksforhold.[50]

4.2.3 Subjektive krav

Tilregnelseskravet for straffelovens § 291 er som udgangspunkt forsæt, jf. straffelovens § 19. Det er dog bestemt i straffelovens § 291, stk. 3, at grov uagtsomhed er tilstrækkeligt, hvis skaden sker under de i stk. 2 nævnte omstændigheder. De subjektive krav til straffelovens § 291 vil i det følgende ikke være genstand for en nærmere analyse.

[48] Straffelovsbetænkning 1923, mot. 383
[49] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 670
[50] RM 9/2005 (under § 291)

4.3 Domsanalyse

I afsnit 4.2.2 er der redegjort for hærværksbestemmelsen i straffeloven. Det er her påvist, at domstolene har anlagt en forholdsvis bred forståelse af ordet ”ting” i straffelovens § 291, stk. 1. I dette afsnit vil det ud fra retspraksis blive undersøgt, om data bliver fortolket i overensstemmelse med ”ting”, og dermed nyder en selvstændig beskyttelse, eller om data er beskyttet ud fra en afledt beskyttelse af det databærende medie.

4.3.1 U.1987.216 Ø (Fagforeningssagen)

4.3.2 Sagens faktum

Det fremgår af dommen, at T1 var tiltalt efter straffelovens § 291, stk. 2, for at have slettet dagpengecheckprogrammet i et EDB-anlæg, som tilhørte Fagforeningen/Arbejdsløshedskassen A. Dette medførte, at A ikke længere kunne udskrive dagpengecheks til A’s medlemmer.

T2 var tiltalt efter straffelovens § 291, stk. 2, for at have flyttet rundt på filer på EDB-anlægget tilhørende A. Flytningen af filerne medførte, at A ikke kunne udskrive breve via EDB-anlægget til A’s medlemmer.

T2 var herudover tiltalt efter straffelovens § 291, stk. 2, ved at oprette og køre et program, som ved start af EDB-anlægget hos A ville slette filerne i EDB-anlægget. Dette skadelige program blev senere automatisk aktiveret, således at filerne på EDB-anlægget blev slettet.

Herudover var T1 også tiltalt for at medvirke til samtlige af T2’s handlinger, da T1 havde givet T2 ordrer til at udfører de omtalte handlinger.

4.3.3 Byrettens afgørelse

I byretten blev T1 og T2 hver især dømt efter straffelovens § 291, da der fandtes at være sket en betydelig skade. Om handlingerne fandt byretten, at de kunne defineres som ødelæggelse, beskadigelse eller bortskaffelse. Således udtalte byretten:

> *”De handlinger, som de tiltalte findes godtgjort at have udført eller have opfordret til at udføre, findes at kunne betegnes som ødelæggelse, beskadigelse eller bortskaffelse i straffelovens § 291's forstand, uanset om der er tale om en sletning, jfr. forholdene 1, 4, 5, 6 og 7, eller en flytning (…)”*[51]

[51] U.1987.216 Ø, side 2

Herudover anførte byretten at EDB-programmer og EDB-registre kan sidestilles med "ting". Dette sker dog kun i kraft af deres umiddelbare tilknytning til det databærende medie.
Retten udtaler:

> *"Retten finder endvidere, at de EDB-programmer og EDB-registre, der under denne sag er blevet slettet eller flyttet, er »ting« i straffelovens § 291's forstand allerede af den grund, at der er sket en beskadigelse af den genstand, der bærer de omhandlede data."*[52]

4.3.4 Landsrettens afgørelse

Det fremgår af dommen, at Landsretten dømmer T1 og T2 efter straffelovens § 291, *stk. 2*, da samtlige handlinger har nødvendiggjort hjælp fra eksterne eksperter.

Ligesom i byretten fandt Landsretten, at data er beskyttet via dens tilknytning til det databærende medie. Herudover fandt landsretten også at der kan være tale om en ødelæggelse af "ting", da det databærende medie ikke kan bruges efter dens formål:

> *"Landsretten finder, at **databærende medier** med **indlagte data** må anses for **»ting«**, således som dette **begreb anvendes i straffelovens § 291**. Såfremt der uberettiget sker sletning af data på datamedier, eller adgangsmulighederne til data i øvrigt uberettiget ændres på en sådan måde, at en hidtidig benyttelse umuliggøres - eller dog kun er mulig for personer med større EDB-indsigt end den sædvanlige bruger – finder landsretten yderligere, at der foreligger »**ødelæggelse**« af en ting, da de databærende medier ikke længere - i hvert tilfælde ikke uden særlige foranstaltninger - kan anvendes efter deres **formål**."*[53] (min fremhævning)

[52] U.1987.216 Ø, side 2
[53] Ibid.

4.3.5 Dommens betydning

I dommen ligger Landsretten op til en afledt beskyttelse af data, da det reelt er det databærende medie, i dette tilfælde EDB-anlægget, som anses for en ”ting”, jf. straffelovens § 291. Dermed beskyttes data i kraft af dets tilknytning til det databærende medie, og deraf er beskyttelsen afledet. Udover at beskyttelsen af data er afledet af det databærende medie anfører Landsretten også, at ødelæggelse af ting foreligger i form af, at det databærende medie ødelægges, og således ikke kan bruges efter dets formål. Landsretten når til denne konklusion på trods af, at det klart fremgår af dommen, at det er data som ødelægges/bortskaffes.

Ud af denne dom kan det ses, at data strafferetligt er beskyttet mod hærværk, men ikke i form af, at data er en ”ting”, jf. straffelovens § 291, stk. 1. Derimod er beskyttelsen afledt af det databærende medie, som data er lagret på.

4.3.6 U.2015.3615 Ø (CSC-sagen)

4.3.7 Sagens faktum

Sagen omhandlede primært hacking, jf. straffelovens § 263, stk. 2, men i sagen forelå der også et eksempel på en ændring i CSC’s systemer, som udgjorde hærværk efter straffelovens § 291. I det følgende vil der primært blive fokuseret på hærværksdelen. Der kan dog i denne sammenhæng ikke ses helt bort fra adgangen til systemet, og dermed hackingdelen. En forudsætning for, at de tiltalte kunne begå hærværk mod data på serveren var, at de først skulle opnå adgang til systemet.

Sagen drejede sig om T1 og T2, som var tiltalt for overtrædelse af bl.a. straffelovens § 291, stk. 2. T1 og T2 havde i forening og på en uberettiget måde, og under skærpende omstændigheder, skaffet sig adgang til et informationssystem, og havde i et stort omfang beskadiget systemet. Systemet tilhørte CSC Danmark A/S. Systemet indeholdt et stort antal data, særligt personfølsomme oplysninger. Disse data tilhørte private og offentlige selskaber, herunder Rigspolitiet.

I første omgang skabte T1 og T2 adgang til CSC’s server ved at udnytte en endnu ukendt sårbarhed i serveren. Herefter blev der oprettet et script (programkode) på serveren, som udgjorde den første ”bagdør”, hvilket vil sige en adgang til serveren udenom de ellers normale sikkerhedsforanstaltninger. Desuden blev der senere tilføjet en linje i en konfigurationsfil, som

dermed udgjorde den anden "bagdør". Formålet hermed var at skabe uautoriseret adgang til CSC' systemer.

4.3.8 Landsrettens afgørelse

Landsretten dømmer T1 for bl.a. hærværk, men frifinder T2 for hærværk, da landsretten vurderer, at han ikke havde andel i at begå hærværk mod systemet.

Landsretten mente, at de oprettede programkoder og ændringen i serverens konfigurationsfil udgjorde hærværk. Således begrundede Landsretten domsfældelsen af T1 med følgende formulering:

> *"Desuden tiltræder vi, at det udgør **hærværk i betydeligt omfang efter straffelovens § 291, stk. 2**, at gerningsmanden i forbindelse med hackerangrebene **oprettede filer med programkoder (scripts) i CSC's system** og foretog **ændringer i internetserverens konfigurationsfil**, hvilket kompromitterede beskyttelsen af de oplysninger, der lå på mainframen, således at enhver med kendskab hertil kunne skaffe sig uberettiget adgang til personfølsomme oplysninger på mainframen."*[54] (min fremhævning)

4.3.9 Dommens betydning

Det skal understreges at størstedelen i denne sag omhandler spørgsmålet om hacking. Således var det kun en mindre del af de begåede handlinger, som udgjorde hærværk. Landsrettens præmisser udgør da heller ikke mere end 8 linjer, men dommen er vigtig, da der muligvis ses en ændring i retspraksis angående beskyttelsen af data.

Landsretten når frem til, at det udgør hærværk, at der blev oprettet filer med programkoder, ligesom ændringerne i serverens konfigurationsfil skulle udgøre hærværk. Det fremgår ikke klart af dommen, om der hermed menes en ødelæggelse, beskadigelse eller bortskaffelse af data.

I modsætning til U.1987.216 Ø (Fagforeningssagen) fokuserer landsretten ikke på det databærende medie (serveren), og dermed på en afledt beskyttelse af data. De fokuserer i stedet for på de ikke autoriserede oprettede filer på serveren, og de ændringer som T1 foretog i serverens konfigurationsfil, således at sikkerheden på serveren blev kompromitteret. I dette

[54] U.2015.3615 Ø, side 7

tilfælde lægger Landsretten derfor umiddelbart op til en selvstændig beskyttelse af data, og anser dermed data som beskyttelsesobjektet for straffelovens § 291. Således kan det muligvis siges at Landsretten fortolker ordet ”ting”, som beskrevet i straffelovens § 291, stk. 1, i overensstemmelse med ordet data. Sagt på en anden måde er fokus flyttet væk fra det databærende medie og hen imod data selv.

Det skal dog fremhæves som en usikkerhedsfaktor, at der af trykte domme kun findes denne ene nyere landsretsdom, ligesom præmisserne angående hærværk er forholdsvis kort begrundede. Herudover kan det tilføjes at anklagemyndigheden valgte at tiltale T1 og T2 ud fra begrundelsen om, at CSC’s informationssystem i betydeligt omfang var blevet beskadiget. Ud fra tiltalen er fokus således stadig rettet mod en afledt beskyttelse af data. Landsretten omtaler dog ikke en beskadigelse af systemet, men fokuserer derimod på ændringen af en konfigurationsfil, som efter Landsrettens opfattelse skulle have kompromitteret beskyttelsen af de oplysningerne, som var lagret på serveren.

4.4 Kommissionsbetænkninger

Der er igennem årende udgivet to betænkninger vedrørende datakriminalitet. Disse betænkninger vil i dette afsnit blive analyseret for at belyse problemstillingen angående den afledte/selvstændige beskyttelse af data.

4.4.1 Betænkning nr. 1032/1985

Justitsministeriet adspurgte i 1984 straffelovsrådet om en udtalelse omhandlende, hvorvidt de dagældende bestemmelser i straffeloven var udformet på en sådan måde, at de kunne anvendes på forbrydelser relateret til datakriminalitet. Dette ledte til straffelovsrådets betænkning nr. 1032/1985 om datakriminalitet. Justitsministeriet mente, at der kunne herske en vis usikkerhed ved anvendelsen af bestemmelserne omhandlende fredskrænkelser, berigelsesforbrydelser, hærværk og brugstyveri set i forhold til datakriminalitet.[55]

Straffelovsrådet indleder med at bemærke, at fysiske ting, såsom et dataanlæg eller et datalagringsmiddel, kan udsættes for hærværk, da disse kan ødelægges, beskadiges eller bortskaffes, og derfor falder ind under straffelovens § 291. Straffelovsrådet henviser til at hærværk af disse ting ikke adskiller fra hærværk af andre fysiske genstande.[56]

Herefter retter straffelovsrådet blikket mod data og om en sletning af data er omfattet af straffelovens § 291:

> *"Det kan diskuteres, om man kan tale om beskadigelse eller ødelæggelse af en "ting", når man alene tænker på det indgreb, der sker i systemets mindste enhed, hvor data lagres ved magnetisering af et felt og kan kaldes frem ved aktivering af dette."*[57]

Straffelovsrådet bemærker herefter, at de finder det sandsynligt, at data vil blive anset for en "ting", som kan beskadiges eller ødelægges, hvis det skulle ende med principiel sag hos domstolene.[58] Dette var dog ikke tilfældet i U.1987.216 Ø (Fagforeningssagen) som refereret ovenfor. Her blev udfaldet en afledet beskyttelse af data. En afledet beskyttelse af data er netop det næste som straffelovsrådet foreslår som en løsning:

[55] Betænkning nr. 1032 (1985), side 64
[56] Betænkning nr. 1032 (1985), side 36
[57] Betænkning nr. 1032 (1985), side 37
[58] Ibid.

> *"Men spørgsmålet er næppe af stor praktisk betydning. Man kan nemlig opfatte forholdet således, at der ved* ***ændring eller slettelse af data*** *sker en* ***beskadigelse af den genstand, som er databærer, f.eks. et bånd eller en diskette****. Den, hvis båndoptagelse af en koncert eller et møde er blevet slettet af en uvedkommende person, vil opfatte båndet som beskadiget eller ødelagt, selv om der er blevet plads til en ny optagelse, og det samme gør sig gældende for den lovlige bruger af et dataanlæg, når et bånd eller en diskette er blevet indholdsmæssigt ændret. Der er derfor efter straffelovrådets opfattelse ingen hindringer for at betragte de her omtalte handlemåder som angreb på "ting"."* [59](min fremhævning)

Dette citat er vigtigt, fordi straffelovsrådet her ligger op til en afledet beskyttelse af data. Det er således ikke dataene i sig selv, som er beskyttet. I stedet vil "tingen", jf. straffelovens § 291, være at anse som det databærende medie. I 1985 angiver straffelovsrådet det databærende medie, som f.eks. et bånd eller en diskette. I nutidens Danmark vil det databærende medie i højere grad kunne anses som f.eks. en server, computer, eller en mobiltelefon, hvorpå data er lagret. Beskyttelsesobjektet er altså det databærende medie frem for data selv. Data vil således kun være at anse som ødelagt mv., fordi det databærende medie er ødelagt. Denne ødelæggelse af det databærende medie sker i kraft af at indholdet, herunder data, bliver slettet. Det databærende medie vil således ikke kunne bruges efter dens formål. Data beskyttes således alene i kraft af, at det er lagret på et medie. Denne opfattelse gav muligvis god mening i 1985, men i dag har data en helt anden betydning i samfundet, og mange vil formentlig anse data som et fænomen, som kræver en selvstændig beskyttelse mod hærværk frem for den noget omstændelige bagvej, som straffelovsrådet ligger op til.
Det er desuden bemærkelsesværdigt, at straffelovsrådet først redegør for, at domstolene ved fremtidige sager formentlig vil fortolke data som værende "ting", men herefter konkluderer at problemstillingen ikke er af væsentlig betydning, da data vil være beskyttet i kraft af det databærende medie. Dette er eksempel på hvordan, det kan være en udfordring at fortolke begrebet data i overensstemmelse med "ting". Den sikre vej for straffelovsrådet i 1985 til, under

[59] Betænkning nr. 1032 (1985), side 37

alle omstændigheder at anse data som værende beskyttet mod hærværk, var således at se data i en meget nær sammenhæng med det databærende medie.

4.4.2 Betænkning nr. 1417/2002

I 1997 blev justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet nedsat. Udvalget afgav deres betænkning i 2002. Udvalget er også benævnt Brydensholt-udvalget. Udvalget blev nedsat for at fremkomme med forslag, der skulle sikre at bestemmelserne i straffeloven angående datakriminalitet var opdaterede og tidssvarende.[60] Lov nr. 352 af 19. maj 2004 blev udarbejdet på baggrund af Brydensholt-udvalgets betænkning om økonomisk kriminalitet og datakriminalitet. I denne lov blev der foretaget en række ændringer, herunder f.eks. straffelovens § 293, stk. 2, som nu også omfatter elektroniske rådighedshindringer. På baggrund af Brydensholt-udvalgets bemærkninger til straffelovens § 291 blev normalstrafferammen i § 291, stk. 1 ændret fra 1 års fængsel til 1 år og 6 måneders fængsel. Den kvalificerede hærværksbestemmelse i stk. 2 blev hævet fra 4 års fængsel til 6 års fængsel.[61] Herudover foreslog Brydensholt-udvalget ikke flere ændringer af straffelovens § 291.

Brydensholt-udvalget starter med at konstatere, at sletning af data vil være omfattet af hærværksbestemmelsen i straffelovens § 291. Dokumentationen herfor er efter udvalgets mening dommen U.1987.216 Ø (Fagforeningssagen).[62]

Når der er tale om virus, som enten sletter, ændrer eller blokerer data, mener udvalget også, at det vil være sandsynligt, at en virus vil kunne udgøre hærværk efter straffelovens § 291, *"fordi den indgår som en del af systemet og dermed ændrer dette."*[63]

Selvom udvalget i det væsentligste finder hærværksbestemmelsen i straffelovens § 291 dækkende, finder udvalget, at *"(…) Dækningen er imidlertid ikke utvivlsom i alle tilfælde, hvilket kan tale for en klar regulering. Dertil kommer, at selv når hærværksbestemmelsen må antages at være anvendelig, ligner den edb-mæssige ødelæggelse i dens forskellige former ikke de ødelæggelser, der kendes fra traditionelt hærværk. Der rejser sig derfor også det principielle*

[60] Betænkning nr. 1417 (2002), side 9-10
[61] Lovbemærkningerne til Lov nr. 352 af 19. maj 2004, side 4
[62] Betænkning nr. 1417 (2002), side 131
[63] Betænkning nr. 1417 (2002), side 136

spørgsmål, om det under alle omstændigheder er hensigtsmæssigt, at straffeloven tilpasses IT-udviklingen også i tilfælde, hvor den kan eller måske kan dække handlingen med den nugældende formulering (…)"[64]

Udvalget ender dog ikke med at finde det nødvendigt, at udarbejde et forslag til en særskilt bestemmelse om datahærværk, da udvalget finder at den nuværende bestemmelse i straffelovens § 291 er dækkende for alle typer af hærværk.

4.5 Ny teknologi

Den teknologiske udvikling har i dag skabt udfordringer for den afledte beskyttelse af data. Den afledte beskyttelse af data fungerer således ikke uproblematisk i sammenhæng med udvikling af ny teknologi, som f.eks. cloud computing.

Cloud computing er en betegnelse for en metode for, hvordan både virksomheder og private i dag lagrer data. Tidligere skete lagringen af data i højere grad lokalt, f.eks. på folks egne bærbare computere eller mobiltelefoner. Virksomheder havde selv mulighed for at lagre data på interne servere. Det var således den samme virksomhed/privatperson, som havde ejendomsretten til både data og det databærende medie (f.eks. server, computer, mobiltelefon).

I dag er det muligt for de samme virksomheder og privatpersoner at gemme og lagre data hos eksterne udbydere af lagringsplads. En sådan udbyder kunne f.eks. være Google, som udbyder en mailtjeneste og desuden skaber mulighed for lagring af fotos og dokumenter. For mobiltelefoners vedkommende kan iCloud anvendes som eksempel. Fælles for disse tjenester er, at lagringen af data sker på en ekstern enhed i form af Google's eller Apple's servere, som kan befinde sig et hvilket som helst sted i verden. Dette kan give visse fordele i form af frigivelse af lagringsplads eller i form af den manglende nødvendighed i overhovedet at være afhængig af sin egen server eller harddisk. Herudover medvirker cloud computing også til at brugerne kan tilgå deres data på flere forskellige enheder over hele verden, så længe der er adgang til en internetforbindelse. Denne nye teknologi er en udvikling, som har medført en øget fleksibilitet, hvad angår tilgangen til data.

[64] Betænkning nr. 1417(2002), side 137

Cloud computing udgør flere problemstillinger rent juridisk. Således medfører teknologien, at det er udbyderen af cloud computing, som har ejendomsretten til det databærende medie, mens det er brugeren, som har ejendomsretten til data. Dette betyder, at en afledt beskyttelse af data vil virke forkert. Er der således et forskelligt ejerforhold over henholdsvis data og det databærende medie, og data herefter udsættes for hærværk, vil det forekomme underligt at lade beskyttelsen angå det databærende medie. I dette tilfælde må det være data, som anses for ødelagt, beskadiget eller bortskaffet.[65]

Helt konkret vil problemet opstå, hvis gerningsmanden til hærværket er den samme som udbyderen. Hvis der f.eks. opstår en tvist mellem Google og brugeren, hvor en medarbejder hos Google begår hærværk mod brugerens data, vil der således ikke være tale om ødelæggelse mv. af en "ting", der tilhører en anden, da ejeren af det databærende medie er Google. Den anden problemstilling ligger i påtalekompetencen, jf. straffelovens § 305, stk. 1.[66] For hærværk begået efter straffelovens § 291, stk. 1, rejses der kun påtale efter forurettedes begæring, medmindre påtale kan ske efter almene hensyn. Det følger således af straffelovens § 305, stk. 1 og retsplejelovens § 725, stk. 1, at fremsættelse af begæring om offentlig påtale tilkommer den forurettede. Det er ikke fastslået ud fra hverken straffeloven eller retsplejeloven, hvem der i straffesager skal anses for den forurettede. Udgangspunktet må dog være, at begrebet "den forurettede" *"(…) omfatter personer, hvis beskyttelse det pågældende straffebud særlig tager sigte på."*[67] Sigtet i straffelovens § 291, stk. 1, er en andens "ting". Forurettede må derfor være den person, som ejer den pågældende "ting".

I forhold til data opstår problemet angående påtalen, jf. straffelovens § 305, stk. 1 således, hvis den fysiske eller juridiske person som har ejendomsretten over det databærende medie ikke vil have sagen undersøgt. Baggrunden for dette kunne være, at det ikke ønskes at gerningsmanden skal findes eller, fordi der ikke ønskes ressourcer afsat til sagens opklaring.[68]

[65] Tfk 2013.240, afsnit 3.1.1.1
[66] Ibid.
[67] Betænkning nr. 1485 (2006)
[68] Tfk 2013.240, afsnit 3.1.1.1

4.6 Delkonklusion

I dette kapitel er straffelovens § 291 blevet præsenteret. Der er her fokuseret på de objektive krav til bestemmelsen, hvor det er klarlagt, at domstolene har anlagt en forholdsvis bred fortolkning af ordet ”ting”. Ordet ”ting”, jf. straffelovens § 291, stk. 1, er i forarbejderne blevet beskrevet som løsøre og fast ejendom. Det er blevet påvist ud fra U.1987.216 Ø (Fagforeningssagen), at data er beskyttet mod hærværk. Denne beskyttelse består dog i en afledt beskyttelse, da det reelt er det databærende medie, som i dommen bliver fortolket i overensstemmelse med tingsbegrebet i straffelovens § 291. I U.2015.3615 Ø (CSC-sagen), er fokus flyttet fra beskyttelsen af det databærende medie. I dommen bliver resultatet, at en ændring af konfigurationsfil og tilføjelse af et program udgør hærværk. Dette peger i retning, af at domstolene har skiftet retning fra den afledte beskyttelse til en selvstændig beskyttelse. Som en forløber til 1987 dommen udgav straffelovsrådet i 1985 deres betænkning om datakriminalitet. I denne betænkning bakker straffelovsrådet op om en afledt beskyttelse, da det databærende medie af straffelovsrådet anses som ødelagt ved en sletning af indholdet. I 2002 udkom Brydensholt-udvalgets betænkning angående IT-kriminalitet. Heri redegør Brydensholt-udvalget for deres syn på straffelovens § 291, og dens anvendelse ved sager, hvor der begås hærværk mod data. Udvalget konstaterer, at hærværk af data i dag kan straffes efter straffelovens § 291 og henviser til U.1987.216 Ø (Fagforeningssagen). Udvalget konkluderer, at der generelt ikke er behov for en ny bestemmelse i straffeloven udelukkende omhandlende hærværk af data. Til sidst i dette kapitel er problemstillingen angående udviklingen af ny teknologi, herunder cloud computing. Det er konstateret, at der består to problemer ved at have en afledt beskyttelse af data. Disse to problemer angår henholdsvis ejerforholdet og påtalereglen i straffelovens § 305, stk. 1. Beskyttelsen af data vil således kun være fyldestgørende, hvis ordet ”ting” i straffelovens § 291 kan fortolkes i overensstemmelse med ordet data. Næste kapitel vil således være genstand for fortolkning af ordet ”ting” i straffelovens § 291, stk. 1, for at undersøge om data kan underlægges en selvstændig beskyttelse.

Kapitel 5
Er data beskyttet som en ting?

Det blev i sidste kapitel analyseret, hvordan data er beskyttet mod hærværk. Både U.1987.216 Ø (Fagforeningssagen) og betænkningerne fra 1985 og 2002 angiver en retning, hvor data har en afledt beskyttelse, fordi data er beskyttet i kraft af det medie, som data er lagret på. Kun U.2015.3615 Ø (CSC-sagen) peger muligvis i en retning, hvor data anses som selvstændigt beskyttet. Som beskrevet i domsanalysen af U.2015.3615 Ø (CSC-sagen), fremgår det dog ikke fuldstændigt klart, om det er data selv som beskyttes, eller om data beskyttes via det databærende medie. Ligeledes er det et usikkerhedsmoment, at der på området angående datahærværk ikke er flere trykte domme, som angiver en retning for domstolenes syn på disse sager. På baggrund af usikkerhed i retspraksis, og fordi en afledt beskyttelse skaber udfordringer ved den teknologi, som i dag eksisterer, vil det være relevant at foretage en analyse af, om begrebet data kan fortolkes i overensstemmelse med begrebet ”ting” i straffelovens § 291, stk. 1. En selvstændig beskyttelse af data vil betyde, at Danmark opfylder kravet i Cybercrime-konventionens artikel 4 om en selvstændig beskyttelse af data. Herudover vil udfordringerne angående Cloud Computing også gøres illusorisk. Ved en selvstændig beskyttelse af data opnås der nemlig adgang for den forurettede til at begære forholdet påtalt. Herudover skal der heller ikke længere skelnes mellem ejerforholdet til henholdsvis det databærende medie og data selv.

En lovfortolkning vil oftest tage udgangspunkt i en præsentation af hele bestemmelsen, i dette tilfælde straffelovens § 291. Hertil henvises der til afsnit 4.1 og 4.2, hvor bestemmelsen er blevet gennemgået, herunder domstolenes normale fortolkning af begrebet ”ting”.

I dette kapitel vil der være en kort gennemgang af, hvordan data kan udsættes for hærværk i form af ødelæggelse, beskadigelse og bortskaffelse. Dette sker, fordi det ikke kun er genstanden ved hærværk, der er vigtig, men også måden, hvorpå data ødelægges mv. Fokus vil dog være på fortolkningen af begrebet ”ting”, da det er her udfordringen ligger ift. hærværk af data.

Hernæst vil tingsbegrebet i straffelovens § 291 blive fortolket. Det vil således først og fremmet blive undersøgt, om der er umiddelbart hjemmel til at idømme straf for hærværk af data efter straffelovens § 291, eller om dette må ske ud fra en udvidet fortolkning/analogi. Straffeloven indeholder ikke en legaldefinition af de forskellige begreber anvendt i loven. Udgangspunktet for en fortolkning af tingsbegrebet vil derfor være en almindelig sproglig fortolkning, men med inddragelse af forarbejder til bestemmelsen. I denne sammenhæng vil tingsbegrebet i straffelovens § 291 blive afgrænset af andre bestemmelser i straffeloven, hvori tingsbegrebet indgår. Tingsbegrebet anvendes også på andre retsområder, og derfor vil tingsbegrebet i medfør af tingsretten også blive undersøgt. Dette sker for at belyse, hvordan en ”ting” defineres i tingsretten. Dette sker ud fra en bevidsthed om, at hensynet bag straffeloven og det at idømme straf ikke er i de samme hensyn, der gør sig gældende ved tingsretten. Der kan formentlig heller ikke være grundlag for at tale om en fælles anvendelse og forståelse af tingsbegrebet i henholdsvis strafferetten som i tingsretten. Dog er tingsbegrebet ikke et særligt strafferetligt udtryk, og derfor vil erfaringer fra tingsretten indgå som et fortolkningsbidrag.

Det er i litteraturen blevet nævnt, at data kan anses for at være en ”ting”, fordi tingsbegrebet skulle kunne fortolkes dynamisk. Det vil derfor også være værd at overveje, om data ud fra en dynamisk fortolkning er direkte omfattet af tingsbegrebet.

Når der i det følgende henføres til tingsbegrebet, henføres der til ordet ”ting”, som det kommer til udtryk i straffelovens § 291, stk. 1.

5.1 Ødelæggelse, beskadigelse, bortskaffelse

Det må som det første afklares, om data kan være udsat for en ødelæggelse, beskadigelse eller bortskaffelse. Hvis data slettes, f.eks. ved at en medarbejder sletter data i virksomhedens kundedatabase, således at denne ikke længere er tilgængelig for hverken virksomheden selv eller virksomhedens kunder, må sletningen kunne sidestilles med ødelæggelse. Det kunne også tænkes at medarbejderen tilføjer urigtige data i virksomhedens database. I dette tilfælde vil der være tale om en beskadigelse.[69] Man vil formentlig også kunne forestille sig, at data kan blive omplaceret internt på en server og dermed blive gjort utilgængeligt for brugerne af serveren. I dette tilfælde kan der blive tale om en bortskaffelse. Det kan således konstateres, at data på lige fod med fysiske ting kan ødelægges, beskadiges eller bortskaffes.

5.2 "Ting"

Ved fortolkningen af tingsbegrebet i straffelovens § 291, stk. 1, kan der tages udgangspunkt i forarbejderne til bestemmelsen. Som tidligere beskrevet er fortolkningsbidraget fra kommissionsbetænkningen af 1923, at tingsbegrebet omfatter fast ejendom og løsøre. Denne betragtning var formentlig fuldt ud dækkende i 1923, da et fænomen som computerdata endnu ikke var opfundet. Nogle vil formentlig mene, at det er mindre brugbart at anvende en snart 100 år gammel straffelovsbetænkning på et område angående data. Data er således et relativt nyt fænomen, som lovgiver og kommisionsmedlemmer ikke har kunnet tage højde for i 1923. Dette synspunkt kan også have en vis mening. Ikke desto mindre har selv ældre forarbejder til straffeloven stadig gyldighed, da bestemmelsen ikke har ændret sig nævneværdigt igennem årene. Tingsbegrebet har således indgået i bestemmelsen helt tilbage fra straffeloven af 1930. Et udgangspunkt for analysen af ordet "ting" må derfor tage sit udgangspunkt i forarbejdernes forståelse af ordet.

Det fremgår dog også af nyere betænkninger på strafferetsområdet, at en "ting" i relation til straffelovens § 291, stk. 1 skal forstås som løsøre. Således fremgår det af straffelovsrådets betænkning fra 1985 om datakriminalitet, at begrebet "ting" i straffelovens § 291 omfatter, *"(…)en*

[69] Tfk 2013.240, afsnit 3

fysisk genstand, d.v.s en genstand man kan tage og føle på(…)".[70] Med denne forståelse af tingsbegrebet er det formentlig heller ikke mærkeligt, at straffelovsrådet i 1985 endte med foreslå en beskyttelse af data igennem det databærende medie. Således vil det være svært at argumentere for, at data bestående af en given mængde tegn, heltal og flydende tal skal kunne defineres som en genstand man kan røre ved.

Det kan i dag antages, at tingsbegrebet fortolkes som en *"afgrænset fysisk størrelse bestående af fast stof der kan ses og røres"*.[71] Ligesom i 1923 og 1985 fortolkes tingsbegrebet i dag som løsøre.

Det næste element bliver derfor at definere, hvad der ligger i ordet løsøre. Ordet har haft en lang fortid i det danske sprog, og kan deles op i løs og øre. "Løs" er lig med bevægelig og "øre" er lig med ejendel.[72] Der er således tale om en bevægelig ejendel, og dermed et objekt som kan flyttes.

Ordet løsøre omfatter f.eks. *"(…)flytbare fysiske formuegenstande, dvs. møbler, husgeråd, maskiner, inventar, varelagre o.l."*.[73] Traditionelt er ordet afgrænset over for fast ejendom og tjenesteydelser.[74] Løsøre er derfor et begreb, der er med til at beskrive ting i den fysiske verden. Det er derfor heller ikke mærkeligt, at ordet "ting" i straffelovens § 291, stk. 1 er blevet fortolket i overensstemmelse med hunde, træer og veje. Disse tre fænomener kan karakteriseres som enten løsøre eller fast ejendom. Spørgsmålet er derfor, om data kan fortolkes i overensstemmelse med tingsbegrebet, når "ting" beskrives som løsøre?

Spørgsmålet besvares forskelligt ud fra, om man anser løsøre som et udtryk for fysiske flytbare genstande eller kun flytbare genstande. I artiklen Tfk2013.240 argumenterer Peter Dueholm Mathiasen, for at data kan anses for løsøre, da data kan flyttes fra én enhed til en anden enhed, f.eks. en computer eller mobiltelefon. Han omtaler også det eksempel, at man i dag fysisk kan medbringe data, hvorhen man vil.[75]

Uanset om data medbringes på en fysisk enhed eller om data opbevares i "skyen" via cloud computing vil data altid være afhængig af et fysisk medie. Selvom data kan sendes via internettet

[70] Betænkning nr. 1032 (1985), side 30
[71] http://ordnet.dk/ddo/ordbog?query=ting&tab=for
[72] http://denstoredanske.dk/Samfund,_jura_og_politik/Jura/Tingsret_og_ejendomsret/l%C3%B8s%C3%B8re
[73] Ibid.
[74] Ibid.
[75] Tfk 2013.240, afsnit 3.1

og opbevares eksternt i "skyen" ligger data således stadig fysisk på f.eks. en server et sted i verden. Data er således ikke bevægelig i en selvstændig form. Dette hænger selvfølgelig sammen med, at data heller ikke er anses som en fysisk ting, som kan røres, da data alene opgøres i tegn, flydende tal og heltal.

Som beskrevet i indledningen til dette kapitel er det relevant at afgrænse straffelovens § 291, stk. 1 over for andre bestemmelser i straffeloven, hvori ordet "ting" indgår. I de følgende afsnit vil det derfor bliver undersøgt, hvordan tingsbegrebet skal fortolkes i medfør af straffelovens § 276 og § 293.

5.2.1 Straffelovens § 276

Straffelovens § 276 er en af de bestemmelser, hvor genstanden i gerningsbeskrivelsen er en "ting". Således omhandler bestemmelsen den person, som har forsæt til at borttage *"en fremmed rørlig ting, for at skaffe sig eller andre uberettiget vinding ved dens tilegnelse."*

Forbrydelsens genstand er en *"fremmed rørlig ting"*. Hermed menes der fysiske "ting" i modsætning til immaterielle værdier. Kopiering af en virksomheds hemmelige formler er således heller ikke tyveri. Ligeledes vil tyveri af en fordring betinges af, at fordringen er knyttet til et fysisk objekt.[76]

Der er flere forskelligheder mellem bestemmelsen i straffelovens § 291 og § 276. I relation til tingsbegrebet er modsætningen, at § 276 nævner en "rørlig ting", mens der i § 291, kun er tale om en "ting". I sammenhæng med ordet rørlig forstås, at tingen skal kunne flyttes. Dette element foreligger allerede ved, at tingen skal kunne borttages.[77] Ved "rørlig ting" må der ikke alene forstås en "ting", men også en fysisk "ting", som kan flyttes.[78] Der skal således være tale om en *"(…) genstand man kan tage og føle på(…)".*[79] Selv uden for de tilfælde, som er omfattet af immaterialretten, vil det derfor også udelukke, at der kan ske tyveri af "ting", som befinder sig i den virtuelle verden, selvom tingen måtte være tillagt økonomisk værdi.

[76] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 587
[77] Gorm Toftegaard Nielsen mfl., Kommenteret straffelov speciel del, side 588
[78] Betænkning nr. 1032 (1985), side 30
[79] Ibid.

Det kan diskuteres, om det skal tillægges værdi, at der i straffelovens § 291 ikke er nævnt, at tingen skal være rørlig. Dette må dog afvises, da ordet ”rørlig” først og fremmest henviser til, at tingen skal kunne borttages. Herudover må det formodes, at man fra lovgivers side i starten af 1900-tallet ikke har villet afgrænse straffelovens § 276 over for data/virtuelle fænomener, da disse ikke fandtes på dette tidspunkt.

Et eksempel på, at ”ting” i relation til tyveribestemmelsen er blevet fortolket i overensstemmelse med en fysisk ”ting” er 2. pkt. i § 276. Heraf fremgår det, at en energimængde, såsom lys, varme, kraft eller bevægelse, skal sidestilles med en ”rørlig ting”. Tyveri af en kabelledning, hvori der transporteres energi, vil klart være omfattet af § 276. En energimængde har dog ikke samme fremtoning som fysiske ”ting”, og derfor har det været nødvendigt at lave en tilføjelse til § 276. Lovgiver har således på dette punkt ment, at der skulle være klar lovhjemmel for tyveri af en ikke fysisk ”ting”.

Med undtagelse af 2. pkt. i straffelovens § 276 kriminalisere tyveribestemmelsen således kun borttagelsen af fysisk rørlige ”ting”.

5.2.2 Straffelovens § 293

Brugstyveribestemmelsen i straffelovens § 293 ligner hærværksbestemmelsen dog med den forskel, at der ved brugstyveri er tale om en uberettiget brug/hindring, mens der ved hærværk er tale om ødelæggelse mv. Forbrydelsens genstand i § 293, stk. 1 og 2 er en ”ting”. Ordet ”ting” skal i § 293 forstås ligesom ordet i § 291, nemlig som enten fast ejendom eller løsøre.[80] Straffelovens § 293, stk. 1 angår den uberettigede brug. Den uberettigede brug af en ”ting” kom til udtryk i U.2003.1950 Ø, hvor en af politiets servere blev benyttet til at opbevare pornografisk materiale. I dommen var det den uberettigede brug af serveren, og dermed en fysisk ”ting”, som der blev lagt vægt på.

Straffelovens § 293, stk. 2 kriminaliserer den uberettigede hindring. Stk. 2 blev ændret i 2004 da man mente, at det kun var de fysiske rådighedshindringer, som var kriminaliseret ifølge bestemmelsen, og dermed ikke også de elektroniske rådighedshindringer.[81] Elektroniske rådighedshindringer kan f.eks. bestå af de tidligere beskrevet DoS-angreb. Et sådant angreb er

[80] Oluf krabbe, Borgerlig straffelov, side 666
[81] Lovkommentaren til lov nr. 352 af 19/05/2004, afsnit 1.2

karakteriseret ved en hindring af serveren ved at serveren bliver overbelastet af uendeligt mange internet-adresse forespørgsler. Således hindres ejeren i at råde over serveren, mens angrebet står på.

På baggrund af at Brydensholt-udvalget i 2002 ikke mente, at der var tilstrækkelig straffemæssig dækning set forhold til ovenstående angreb, blev straffelovens § 293, stk. 2 ændret fra "lægger hindringer i vejen" til "uberettiget hindrer". Dette blev gjort for at understrege, at der ikke kræves en fysisk hindring for at bestemmelsen er anvendelig, når hindringen har karakter af en elektronisk rådighedshindring.[82]

Selvom bestemmelsen nu også vedrører hindringer forårsaget af elektronisk vej er det stadigvæk i IT-mæssigt sammenhæng hindringen af systemet (f.eks. en server), der er genstand for forbrydelsen og dermed en fysisk "ting", som beskyttes mod en uberettiget hindring.

5.2.3 Tingsretten

I tingsretten skelnes der traditionelt mellem fysiske og ikke fysiske "ting". Hermed sigtes der til en opdeling af "ting", som henholdsvis har en fysisk substans, herunder fast ejendom og løsøre og "ting", som ikke har fysisk udstrækning, f.eks. patentrettigheder.[83] I tingsretten bliver "ting" således afgrænset på samme måde, som straffelovskommissionerne i 1923 og 1985 afgrænsede begrebet, nemlig som fast ejendom og løsøre. I tingsretten skelnes der mellem almindeligt løsøre og motorkøretøjer, skibe og fly, som anses for en særskilt type af løsøre. Det almindelige løsørebegreb afgrænses derfor negativt over for motorkøretøjer, skibe og fly. Således kan løsøre i tingsretten afgrænses som alle fysiske "ting", som ikke er *"motorkøretøjer, skibe(...), luftfartøjer, fast ejendom(..)"*.[84] I tingsretten skelnes der således mellem "ting" af fysisk karakter og "ting" af ikke fysisk karakter, som dermed ikke er omfattet af reglerne for løsning af tredjemandskonflikter.

[82] Betænkning 1417 (2002)
[83] Peter Mortensen, Indledning til Tingsretten, side 36
[84] Peter Mortensen, Indledning til Tingsretten, side 46

5.2.4 Dynamisk fortolkning af ting

Det har været angivet i litteraturen, at tingsbegrebet kan fortolkes dynamisk, således at tingsbegrebet skal forstås i overensstemmelse med den teknologiske udvikling i samfundet. Peter Dueholm Mathiasen har skrevet en artikel om den strafferetlige beskyttelse af data og mener at tingsbegrebet skal fortolkes dynamisk og henviser til en ældre ordbogsbetegnelse af tingsbegrebet, *"Begrebet »ting« bliver almindeligvis anvendt om »enkeltfænomener uden hensyn til dets (abstrakte ell. konkrete) væsen […]; ofte om hvad man ikke kan ell. vil angive nærmere«.(…) Hvis en sådan forståelse af begrebet accepteres, er der tale om et dynamisk begreb, og der er således plads til en gradvis retsudvikling i takt med teknologiske nyskabelser."*[85] Mathiasen mener, at der ud fra ordbogsbetegnelsen kan udledes, at tingsbegrebet kan fortolkes dynamisk. Dette skulle sikre, at der er rum for en vis retsudvikling i overensstemmelse med den nye teknologi, som hen ad vejen måtte opstå.[86]

Inge Marie Sunde har behandlet det norske tingsbegreb i relation til reglerne om beslaglæggelse i den norske straffelov. Hun mener i overensstemmelse med Peter Dueholm Mathiasen, at tingsbegrebet må kunne fortolkes dynamisk, fordi ordet "ting" er et generelt udtryk, og derfor skal anses for at være tidsbestandigt.[87]

Den dynamiske fortolkning kendes især fra den Europæiske Menneskerettighedsdomstol og er derfra kendetegnet, som en fortolkningsstil, som skal fortolke den Europæiske Menneskerettighedskonvention ud fra "present days conditions". I dansk ret, herunder strafferetten, er der som udgangspunkt ikke tradition for at anvende denne fortolkningsstil. Fortolkningsstilen må tage udgangspunkt i de traditionelle fortolkningsprincipper. Således må der tages udgangspunkt i en subjektiv eller objektiv fortolkning, herunder indskrænkende, præciserende eller udvidende fortolkning (analogi). Dette må ikke mindst gælde inden for strafferetten, da der kræves lovhjemmel for at idømme straf, jf. straffelovens § 1. Udtrykket dynamisk fortolkning kan muligvis anses som en udvidende fortolkning. Ved udvidende fortolkning må der dog tages udgangspunkt i bl.a. formålet med bestemmelsen fremfor en henvisning til en historisk ordbogsbetegnelse.

[85] Tfk.2013.240, afsnit 3.1
[86] Ibid
[87] Inger Marie Sunde, Automatiseret inndragning, side 119

5.2.5 Straffelovens § 171

Straffelovens § 171 straffer den ”*der gør brug af et falsk dokument til at skuffe i retsforhold”.* Denne bestemmelse nævner ikke ordet ”ting”, men bestemmelsen blev i 2004 ændret således, at den nu også omhandler elektroniske dokumenter. Bestemmelsen kan således ikke bruges som et fortolkningsbidrag til, hvordan ordet ”ting” skal forstås. Straffelovens § 171 er dog et eksempel på en bestemmelse i straffeloven, som tidligere kun angik fysiske dokumenter, men som er blevet ændret med det formål at beskytte elektroniske dokumenter.

Før ændringen i 2004 omfattede straffelovens § 171, stk. 2 kun skriftlige dokumenter. Ved ændringen blev også elektroniske dokumenter omfattet. Denne ændring skete på baggrund af Brydensholt-udvalgets bemærkninger i deres betænkning fra 2002. Udvalget lagde vægt på udviklingen i samfundet, som er gået fra en primær brug af fysiske dokumenter til i højere grad at omfatte elektroniske dokumenter.[88] Således mente udvalget: *”Med den udvikling, der har været siden 1985, og den, der må forventes vide-re frem, er det nærliggende at etablere et strafferetligt værn omkring dataop-lysninger, der erstatter dokumentanvendelse.”*[89]

Brydensholt-udvalget overvejede, angående den tidligere formulering af straffelovens § 171, stk. 2, om ordet ”skriftlig” kunne ændres til ”læsbar”, for derfor at omfatte elektroniske dokumenter. Udvalget fandt dog at dette var utilstrækkeligt set i forhold til bestemmelsens historiske anvendelse ved brug af falske skriftlige dokumenter. Til stk. 2, blev der derfor tilføjet elektronisk dokument.[90]

Ændringen af straffelovens § 171, stk. 2 har dermed vist, at den teknologiske forandring i samfundet har nødvendiggjort en ændring af dokumentfalskbestemmelsen.

[88] Betænkning 1417 (2002), side 118
[89] Ibid.
[90] Betænkning 1417 (2002), side 119

5.2.6 Straffelovens § 263, stk. 2

Straffelovens § 263, stk. 2 omhandler *"den der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem".* Bestemmelsen er placeret i straffelovens kapitel 27, og angår beskyttelsen af privatlivets fred. Som ved straffelovens § 171, indgår ordet "ting" ikke i gerningsbeskrivelsen i § 263, stk. 2. Men som det også var tilfældet med § 171 er § 263 blevet opdateret for at følge med den teknologiske udvikling.

Straffelovsrådet mente således ikke i 1985, at der var tilstrækkelig hjemmel til at straffe en uberettiget adgang til dataanlæg og data.[91] Problematikken var her igen et opgør mellem gamle straffebestemmelser og ny teknologi. Således bestod gerningsindholdet i den ældre bestemmelse i § 263 af f.eks. at bryde et brev eller skaffe sig adgang til andres gemmer, men ikke en egentlig beskyttelse af afgangen til andres oplysninger eller programmer.

I sin betænkning fra 1985, forsøgte straffelovsrådet at klargøre om en beskyttelse af andres oplysninger eller programmer kunne retfærdiggøres ud fra den daværende § 263. Straffelovsrådet mente, at den daværende § 263, nr. 1, (skaffe sig adgang til en "lukket meddelelse") kunne fortolkes således, at den information, som sendes via et dataanlæg, kan siges at udgøre en "lukket meddelelse". Således ville der være strafferetlig dækning for den som uberettiget kobler sig på (hacker) en sådan transmission, hvor information bliver sendt fra et sted til et andet, og gør sig bekendt med den lukkede meddelelse.[92]

Efter straffelovsrådets opfattelse opstod problemet, dog for så vidt angår de informationer, som ikke sendes, men som er opbevaret i et dataanlæg. I denne sammenhæng mente straffelovsrådet ikke, at det ud fra naturlig sporlig forståelse ville være tale om lukkede meddelelser.[93]

Heller ikke det at skaffe sig adgang til andres gemmer var umiddelbart en mulighed. Således udtalte straffelovsrådet, "*Det kan derimod diskuteres, om det ligger inden for den sprogligt naturlige forståelse af ordet "gemme" at anse et dataanlæg som et "gemme" for de deri lagrede informationer."*[94] For straffelovsrådet fremgik det klart, at "en andens gemmer" kunne omfatte

[91] Betænkning 1032 (1985), side 22
[92] Ibid.
[93] Betænkning 1032 (1985), side 22-23
[94] Betænkning 1032 (1985), side 23

traditionelle gemmer, såsom skuffer o.l. Straffelovsrådet mente dog, at et nyere fænomen, såsom et dataanlæg, ikke kunne anses som et gemme for lagrede informationer. Løsningen på dette problem var derfor at lave en tilføjelse til straffelovens § 263 således, at der nu også var klar lovhjemmel til at straffe en uberettiget "adgang til en andens oplysninger eller programmer".

5.2.7 Udvidende fortolkning af tingsbegrebet

Det må baggrund af ovenstående konstateres, at data ikke kan være direkte omfattet af tingsbegrebet i straffelovens § 291, stk. 1. Ordet "ting" har således en naturlig ordgrænse, som data ikke kan være omfattet af. Hverken forarbejderne til § 291, forståelsen af andre bestemmelser i straffeloven, hvor ordet "ting" indgår, den naturlige sporlige forståelse af ordet "ting", som værende løsøre, eller begrebet løsøres forståelse i tingsretten, kan medvirke til en retstilstand, hvor data er direkte omfattet af straffelovens § 291, stk. 1.

Det næste punkt vil være at undersøge om data ud fra en fuldstændig lovanalogi af straffelovens § 291, stk. 1 kan være sidestillet med tingsbegrebet, således at data opnår en selvstændig beskyttelse mod hærværk. Den fuldstændige lovanalogi er tidligere anvendt i strafferetten, om end det forekommer forholdsvist sjældent. Som beskrevet i kapitel 1 er der formel hjemmel i straffelovens § 1 til at fortolke en bestemmelse ud fra en fuldstændig lovanalogi.

Ved domstolenes behandling af sager, hvor den fuldstændige lovanalogi er taget i brug, er der især lagt vægt på formålet med den pågældende bestemmelse, ligesom det har været afgørende, at det pågældende forhold har kunne sidestilles med de af bestemmelsen omfattede forhold.

Formålet med straffelovens § 291 er at beskytte "ting" mod ødelæggelse, beskadigelse eller bortskaffelse. De formuegoder som folk er i besiddelse af skal altså beskyttes mod tredjemands destruerende indgriben. Som det allerede er beskrevet, stammer straffelovens § 291 i dens nuværende form helt tilbage fra straffeloven af 1930. Det er klart at lovgiver ikke i 1930 har kunnet forudse den udvikling, der i dag har fundet sted med hensyn til udvikling af ny teknologi. Da bestemmelsen blev udformet i 1930 blev ordet "ting" formentlig anvendt for at ramme en så bred skare af de formuegoder, som man på dette tidspunkt kendte til. I dag har den teknologiske udvikling dog medført nye fænomener, som ikke længere kan anses for at henhøre under kategorien løsøre.

Selvom data ikke er løsøre, og dermed falder ind under tingbegrebet, har data som formuegode et lige så stort behov for beskyttelse mod hærværk, som det gælder for løsøre. I dag vil de færreste mennesker formentlig mene, at der er forskel på at ødelægge et fysisk brev eller bog og så den situation, hvor en mail eller anden form for data bliver slettet. I begge situationer vil der ske en ødelæggelse/beskadigelse af noget, som en anden person har ejendomsretten over.

I U.1987.216 Ø (Fagforeningssagen) blev data slettet i et betydeligt omfang. Det var derfor egentlig data, som var genstand for forbrydelsen, men Landsretten nåede altså frem til, at det var databærende medie, som havde lidt skade. Da data og det databærende medie, i dette tilfælde var ejet af den samme juridiske person, var der ikke noget problem i at beskytte det databærende medie og data under ét. Dette bliver dog sat på spidsen, når det databærende medie og data ikke ejes af den samme person/selskab. Det er temmelig vanskeligt at se, hvorfor der skal være forskel på disse to situationer, hvor ejerforholdet er ens, og hvor det ikke er. Det bør således ikke fremstå tilfældigt, om der kan straffes for hærværk af data ud fra, hvordan ejerforholdet over henholdsvis data og det databærende medie ser ud.

Data må i høj grad kunne sidestilles med ”ting” i form af løsøre. Der er således ikke en egentlig forskel i beskyttelsesinteressen, hvad angår data og ”ting”. Kun den ydre skikkelse adskiller data og ”ting” fra hinanden. Denne forskel er dog mere eller mindre ubetydelig set i forhold til, hvad der efter straffelovens § 291 forsøges beskyttet. En afvisning af en udvidende fortolkning, i form af en fuldstændig lovanalogi, vil derfor komme til at fremtræde formalistisk. Ved en udvidet fortolkning af tingsbegrebet i straffelovens § 291, stk. 1 vil data kunne anses som værende fyldestgørende beskyttet mod hærværk, særligt i relation til udviklingen af ny teknologi. Da beskyttelsen af data må fortolkes ud fra en udvidende fortolkning af tingsbegrebet i straffelovens § 291, stk. 1, vil lovhjemlen i straffeloven dog ikke fremstå tydelig.

Som det fremgår ovenfor, har lovgiver sørget for at ændre flere bestemmere i straffeloven på baggrund af teknologiens udvikling. Således omfatter straffelovens § 171 om dokumentfalsk, nu også elektroniske dokumenter, ligesom indførelsen af § 262 om hacking har gjort det unødvendigt at bedømme tilfælde af hacking på baggrund af en analogi af den tidligere formulering af § 263.

Den primære grund til at straffelovens § 291 endnu ikke har været genstand for en sproglig opdatering skal formentlig findes i, at der gennem tiden har været henvist til straffelovsrådets

betænkning fra 1985 og dommen U.1987.216 Ø (Fagforeningssagen), hvor data har en afledt beskyttelse. Det vil derfor for mange formentlig fremstå som selvfølgelighed at data er beskyttet mod hærværk. Den afledte beskyttelse af data vil dog i dag ikke fremstå som en god løsning set i forhold til brug af cloud computing. Kun en udvidende fortolkning af tingsbegrebet i straffelovens § 291, stk. 1 vil her kunne betyde, at det vil være strafbart at begå hærværk mod data.

5.2.8 Delkonklusion

Det er i dette kapitel blevet undersøgt, hvorvidt data kan fortolkes i overensstemmelse med tingsbegrebet, og dermed anses for at have en selvstændig beskyttelse mod hærværk. I de situationer, hvor der er anvendt cloud computing, og hvor data og det databærende medie ejes af forskellige aktører, er den selvstændige beskyttelse af data, en nødvendighed. Med udgangspunkt i betænkninger fra 1923 og 1985 skal tingsbegrebet forstås som løsøre. Den naturlige sproglige forståelse af tingsbegrebet vil i dag også rette sig mod løsørebegrebet. Løsørebegrebet er traditionelt fortolket som en fysisk ejendel, som kan flyttes. Ligeledes er tingsbegrebet i straffelovens § 291, stk. 1 afgrænset ud fra andre bestemmelser i straffeloven. Denne afgrænsning har vist, at tingsbegrebet generelt retter sig mod en fysisk ”ting”. Data vil således ikke være direkte omfattet af straffelovens § 291, stk. 1. Det er forsøgt afklaret, om data vil have en beskyttelse mod hærværk ud fra en udvidende fortolkning af hærværksbestemmelsen. Dette er centralt for problemstillingen omhandlende, hvordan data i dag lagres eksternt hos andre, således at ejerforholdet til henholdsvis data og det databærende medie er forskelligt. Det er konstateret, at data formentlig vil være selvstændigt beskyttet mod hærværk ud fra en fuldstændig lovanalogi af bestemmelsen i straffelovens § 291, stk. 1. Her er der særligt lagt vægt på formålet med bestemmelsen og at data i høj grad må kunne sidestilles med ”ting”, da det kun er den ydre skikkelse som adskiller data og ”ting”. Hvis en udvidende fortolkning af tingsbegrebet lægges til grund, vil data også være beskyttet i de tilfælde, hvor der gøres brug af cloud computing. Denne beskyttelse vil dog i sidste ende hvile på en fuldstændig lovanalogi.

Kapitel 6
Konklusion

Samfundet ændrer sig i dag hastigt, og det samme gør den teknologi, som mange i dag er dybt afhængige af. Spørgsmålet er om straffeloven i dag har fulgt med den teknologiske udvikling således, at der er strafferetlig hjemmel til at dømme i sager angående datahærværk. Det er særdeles vigtigt, at der i strafferetten er hjemmel til at dømme, da straf kun kan idømmes for et forhold som er hjemlet ved lov, jf. straffelovens § 1. I denne afhandling har det derfor været et centralt emne at undersøge, hvordan data er beskyttet mod hærværk, og hvordan denne beskyttelse harmonerer med udviklingen af ny teknologi.

Data har i dag som minimum en afledet beskyttelse mod hærværk. Data kan således siges at være beskyttet gennem det databærende medie, hvorpå data er lagret. Dette udledes først og fremmest af dommen U.1987.216 Ø (Fagforeningssagen), som viser at data ikke er genstand for selvstændig beskyttelse. Ved en ødelæggelse af det databærende medie vil dette medie således ikke kunne anvendes efter dets formål. Også betænkninger fra 1985 og 2002 bakker op om den afledet beskyttelse af data. Således har hverken domstolene eller straffelovsrådet/Brydensholt-udvalget været villige til at fortolke data i overensstemmelse med tingsbegrebet i straffelovens § 291, stk. 1.

Udover at data har en afledet beskyttelse mod hærværk kan dommen U.2015.3615 Ø (CSC-sagen) muligvis tages til indtægt for, at data i dag har en selvstændig beskyttelse mod hærværk. I dommen lægges der således vægt på, at det udgør hærværk, at der blev ændret i en konfigurationsfil, ligesom oprettelsen af programkoder på serveren også udgjorde hærværk. Fokus på det databærende medie er således ikke tilstede, som det var tilfældet i U.1987.216 Ø (Fagforeningssagen). Det kan dog ikke ud fra et sikkert grundlag afgøres, om data set ud fra retspraksis er selvstændigt beskyttet. Således er præmisserne ikke særligt uddybende, ligesom det tæller med, at anklagemyndigheden rejste tiltale for overtrædelse af straffelovens § 291 ved at tiltalte havde beskadiget systemet. En beskadigelse af systemet peger igen i retning af en afledet beskyttelse af data.

Det kan således konkluderes at data i dag som minimum er beskyttet mod hærværk gennem en afledet beskyttelse af det databærende medie.

Ud over at afklare, hvordan data i dag er beskyttet, har det også været afgørende at undersøge, om data er fyldestgørende beskyttet, når der anvendes ny teknologi, i form af f.eks. cloud computing. Således vil en afledet beskyttelse af data medføre problemer, hvor ejerforholdet mellem data og det databærende medie er forskelligt. Påtalespørgsmålet og begrebet ”en andens ting” vil således være problematiske elementer i en afledet beskyttelse af data.

Spørgsmålet er derfor, om data kan fortolkes i overensstemmelse med tingsbegrebet i straffelovens § 291, stk. 1. Det fremgår både af forarbejderne til § 291 og betænkningerne på området for datakriminalitet, at tingsbegrebet skal opfattes som enten fast ejendom eller løsøre. En naturlig sproglig forståelse af tingsbegrebet medfører også, at begrebet anses for at omhandle løsøre. Løsøre er normalt betegnet som en fysisk flytbar ejendel. Hvad angår løsøre skelnes der i tingsretten også mellem fysiske og ikke fysiske ”ting”. Det er svært at forene data med en fysisk ”ting”, da data i bund og grund er bestående af tegn, heltal og flydende tal. Data kan derfor ikke ud fra en præciserende ordlydsfortolkning kategoriseres til at være en ”ting”. Dette resultat understreges også ved, at ordet ”ting”, i medfør af straffelovens § 276 og § 293, heller ikke angår andet end fysiske ”ting”.

Det er herefter undersøgt om data, ud fra en fuldstændig lovanalogi, kan være sidestillet med tingsbegrebet. Data vil som udgangspunkt have en selvstændig beskyttelse og være omfattet af straffelovens § 291, stk. 1, da formålet med beskyttelsen af fysiske ”ting” må være den samme ved beskyttelsen af data. Ligeledes må data og ”ting” kunne sidestilles, da det kun er den ydre form, som adskiller de to fænomener. Således vil det fremstå formalistisk ikke at beskytte data mod hærværk på højde med fysiske ”ting”.

Det kan således konkluderes, at den strafferetlige beskyttelse af data formelt set er fyldestgørende i relation til udviklingen af ny teknologi, da data ud fra fuldstændig lovanalogi kan sidestilles med tingsbegrebet i straffelovens § 291, stk. 1. Da der i medfør af straffelovens § 1 er hjemmel til at henføre et forhold under en fuldstændig lovanalogi, skabes der mulighed for i denne sammenhæng at beskytte data selvstændigt.

Det kan dog diskuteres om en beskyttelse af data ud fra en fuldstændig lovanalogi er ønskværdigt. Selvom der er formel hjemmel til at henføre et forhold under en fuldstændig lovanalogi, jf. straffelovens § 1, er analogien ikke hyppigt brugt, formentlig set ud fra et retssikkerhedsmæssigt synspunkt.

Kapitel 7
Perspektivering til norsk ret

I Norge har man også diskuteret problemstillingen angående hærværk af data. I 1985 udgav det norske straffelovsråd betænkning NOU 1985:31, som på mange punkter er en næsten tro kopi af den danske betænkning fra 1985. I den norske betænkning angik spørgsmålet også, om data er beskyttet mod hærværk. Det fremgår i betænkningen, at data ikke kan anses for i sig selv at være en genstand. Således henføres der til, at en "ting", efter en almindelig sproglig forståelse, må være en fysisk "ting". Til støtte for den manglende fysiske beskaffenhed anføres det i betænkningen, at den information, som dataene udgør, har en immateriel form. Det norske straffelovsråd angiver hernæst, at en genstand må opfattes som en løsøregenstand. I norsk ret omfatter en løsøregenstand også lys, varme eller en bevægelse. Det anføres dog at data, ikke kan sammenlignes med en af disse energiformer. Straffelovsrådet anerkendte dog, at der er et åbenlyst behov for at beskytte data mod hærværk. Da data ikke kan være en "ting" i norsk ret, mente det norske straffelovsråd, at den afledte beskyttelse af data kan anvendes som værn mod datahærværk. Straffelovsrådet mente således, at når data slettes eller ændres bliver det databærende medie skadet. [95] Løsningen blev således den samme, som det danske straffelovsråd kom frem til i 1985.

I 2002 blev der i Norge nedsat et udvalg, som skulle gennemgå eventuelle lovtiltag mod datakriminalitet. I 2007 udgav udvalget deres betænkning på området.[96] Udvalget henførte til gældende ret i Norge, hvor data var beskyttet mod hærværk, men hvor denne beskyttelse var en afledt beskyttelse via det databærende medie. For at yde et selvstændigt værn mod datahærværk, stillede udvalget forslag til særskilt bestemmelse omhandlende datamodifikation.[97]

[95] NOU 1985:31, afsnit 4.3
[96] NOU 2007:2, forord
[97] NOU 2007:2, afsnit 5.6.3

Udvalgets forslag til en ny bestemmelse lød:

"For datamodifikasjon straffes den som uberettiget endrer, ødelegger, sletter eller skjuler andres data."[98]

Ifølge udvalget vil enhver ødelæggelse, sletning, eller det at skjule data, anses for at være en ændring. En ændring kan f.eks. ske ved, at data som styrer edb-systemet ændres. En ændring, som rammer filer på edb-systemet således, at sikkerhedsfunktion på edb-systemet sættes ud af kraft, også kunne karakteriseres som en ændring.[99]

Man endte dog ikke med særskilt bestemmelse omkring datahærværk i Norge. Justis- og politidepartementet mente således ikke, at der var behov for en særskilt bestemmelse. Selv om midlet/målet for den strafbare handling er anderledes ved datahærværk er dette ikke tilstrækkeligt til at forsvare en selvstændig bestemmelse. Ikke desto mindre er departementet enig med straffelovsudvalget i, at straffeansvaret for hærværk af data bør tydeliggøres. Det er således utilfredsstillende, at der i tilfælde af datahærværk skal ske fortolkning af den almindelige hærværksbestemmelse, som ikke er tydelig i dens ordlyd hvad angår data. Den almindelige hærværksbestemmelse er således ikke tilstrækkelig anvendelig i de tilfælde, hvor data er udsat for hærværk.[100]

Hærværksbestemmelsen i den norske straffelov, lyder i dag:

"Med bot eller fengsel inntil 1 år straffes den som skader, ødelegger, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen.

For skadeverk straffes også den som uberettiget endrer, gjør tilføyelser til, ødelegger, sletter eller skjuler andres data."[101] (min understregning)

Med denne tilføjelse til hærværksbestemmelsen i den norske straffelov er data i dag selvstændig beskyttet mod hærværk i Norge. Dette betyder, at der i Norge er klar lovhjemmel til at straffe hærværk af data, også i de tilfælde hvor ejerforholdet mellem data og det databærende medie, er forskelligt.

[98] NOU 2007:2, afsnit 11.1 - §7
[99] NOU 2007:2, afsnit 5.6.3
[100] Ot.prp. nr.22 (2008-2009), afsnit 2.15.5
[101] LOV-2005-05-20-28

Ligeledes deltager Norge i Cybercrime-konventionen og har nu tydeliggjort, at data er selvstændigt beskyttet mod hærværk og opfylder derfor konventionens artikel 4.

Kapitel 8
Abstract

This thesis regards how data is protected against vandalism, according to section 291(1) of the Danish Criminal Code. Furthermore, it is discussed in the thesis if the protection against vandalism is adequate, especially in relation to the development of new technology. As a result, thereof, it is investigated if data has an independent protection against vandalism or if the protection is secondary to the data-carrying medium. Based on case law and the preliminary work it is found that data as a minimum is protected secondary to the data-carrying medium. In addition to this, it is seen in case law that the protection of data possibly is going towards an independent protection of data.

New technology has today made It necessary for data to have an independent protection against vandalism. It is examined if the term data can be interpreted in agreement with the term “thing”, according to the Danish Criminal Code section 291(1). This is done from the preliminary work, a well-known understanding of the term “thing”, and a demarcation of the term “thing” by comparing it to other legislative measures in the Danish Criminal Code. It is found that data is not fully covered by section 291(1) of the Danish Criminal Code because the term “thing” must mean a physical movable object. Finally, it is found that the term “thing” is covered by section 291(1), through an analogy. This is based on the purpose of the protection of the term “thing” and data is the same. It can also be stated that the term “thing” and data can be compared, based on the appearance of the two phenomena.

Litteraturliste

Litteratur:

Munk-Hansen, Carsten, Retsvidenskabsteori, 1. udgave, Jurist- og Økonomforbundets Forlag, 2014.

Baumbach, Trine, Det strafferetlige legalitetsprincip, 1. udgave, Jurist- og Økonomforbundets Forlag, 2008.

Waaben, Knud, Strafferettens almindelige del Ansvarslæren, 6. udgave, Karnov Group, 2015.

Bryde Andersen, Mads, IT-retten, 2 udgave, Gads Forlag, 2005.

Greve, Vagn mfl., Kommenteret straffelov almindelig del, 10. udgave, Jurist- og Økonomforbundets Forlag, 2013.

Trzaskowski, Jan mfl., Internetretten, 2. udgave, Ex Tuto Publishing, 2012.

Toftegaard Nielsen, Gorm mfl., Kommenteret straffelov speciel del, 11. udgave, Jurist- og Økonomforbundets Forlag, 2017.

Vestergaard, Jørn, Forbrydelser, 2. udgave, Gads Forlag, 2013.

krabbe, Oluf, Borgerlig straffelov, 3. udgave, Gads Forlag, 1941.

Mortensen, Peter, Indledning til Tingsretten, 2. udgave, Thomson Reuters, 2010.

Marie Sunde, Inger, Automatiseret inndragning, doktorafhandling, 2010.

Artikler:

Tfk 2013.240

Love:

LBK nr. 977 af 09/08/2017 (straffeloven)

LBK nr. 38 af 05/01/2017 (færdselsloven)

BKI nr. 12 af 15/03/2007

LBK nr. 750 af 19/10/1998 (EMRK)

Lov nr. 352 af 19/05/2004

LOV-2005-05-20-28 (norske straffelov)

Europarådets konvention om IT-kriminalitet af 23. november 2001 (Cybercrime-konventionen)

Rammeafgørelse 2005/222/RIA

Betænkninger:

Straffelovsbetænkning af 1923

Betænkning nr. 1032 (1985)

Betænkning nr. 1417 (2002)

Betænkning nr. 1485 (2006)

NOU 1985:31

NOU 2007:2

Ot.prp. nr.22 (2008-2009)

Web-adresser:

http://denstoredanske.dk/It,_teknik_og_naturvidenskab/Informatik/Software,_programmering,_internet_og_webkommunikation/data (sidst besøgt 10/5)

https://ordnet.dk/ddo/ordbog?query=%C3%B8del%C3%A6gge (sidst besøgt 10/5)

http://denstoredanske.dk/Samfund,_jura_og_politik/Jura/Tingsret_og_ejendomsret/l%C3%B8s%C3%B8re (sidst besøgt 10/5)

https://ordnet.dk/ddo/ordbog?query=ting&tab=for (sidst besøgt 10/5)

Domme:

U 1940.156 Ø

U.1960.746/2 B

U 1965.535 V

U.1975.972 V

U 1987.216Ø

U 1996.356 Ø

U 2000.1450 Ø

U 2003.1950 Ø

U 2006.21.68 Ø

U 2015.3615Ø

TfK.2011.668 V

Østre Landsrets dom af 13. februar 1995

Meddelelser:

RM 9/2005

Dokumentation af antal anslag:

DATAHÆRVÆRK

En analyse af den strafferetlige beskyttelse af data