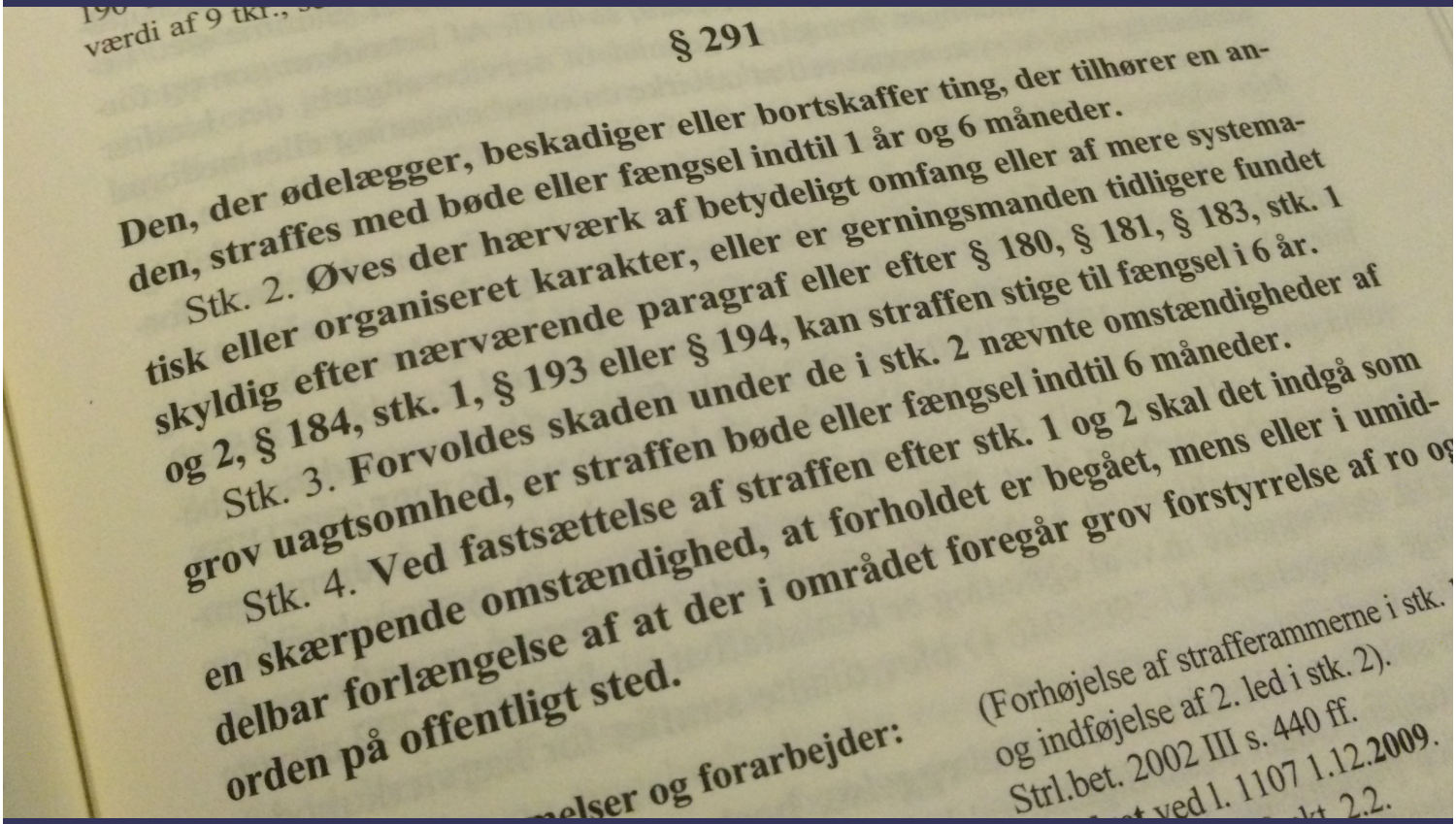
PETER STEENBERG

Datahærværk

- er data en ting?



Kandidatspeciale ved Aalborg Universitet 2015

Titelblad

Uddannelsessted:	Aalborg Universitet, jura
Vejleder:	Lars Bo Langsted
Ekstern vejleder:	Lene Lentz ved anklagemyndigheden
Projekt:	Kandidatspeciale
Emne:	IT-kriminalitet
Titel:	Datahærværk
Titel på engelsk:	Data vandalism
Afleveringsdato:	12. Maj 2015, kl. 10.00
Sidetal:	57 normalsider (137.621 tegn)
Forfatter:	Peter Steenberg

_____

Peter Steenberg, 2009-2982

Indholdsfortegnelse

1. DET INDLEDENDE AFSNIT

1.1 Indledning

De sidste mange år har været præget af en stærk udvikling indenfor informationsteknologi. Internettet havde sine første skridt i starten af 80'erne, og senere blev den personlige computer en del af hverdagen til blandt andet tekstbehandling og til underholdning. Informationsteknologien har i lige så høj grad fundet sit indpas i erhvervslivet, som i højere grad behandler og gemmer sine data digitalt, og i den virtuelle verden formidler og forhandler informationer og programmer, som er udviklet af denne data. Den digitale udviklingen præger samfundet. Efterspørgsel på information og viden stiger i takt med udviklingen, og løsninger som tidligere fungerede analogt, foregår nu digitalt. Post mellem borger og det offentlige foregår i højere grad digitalt, og er bare ét eksempel på den teknologiske udvikling.

Med en sådan udvikling og integrering af informationsteknologi i vores samfund, er der opstået en helt ny verden af muligheder. Muligheder for at kommunikere med hinanden, at lagre information digitalt, og generelt bare at gøre hverdagen lettere, både i privat- og erhvervslivet. Den nye virtuelle verden har dog i lige så høj grad en svaghed, fordi de kriminelle også ser en verden af muligheder. Hvor det tidligere har været svært og at bryde ind og finde den eftertragtede information, giver udviklingen en mulighed for den kriminelle, at udnytte en brugers tillid til informationssystemet, og dermed uberettiget skaffe sig adgang til, eller beskadige de værdifulde data.

IT-kriminalitet er som udgangspunkt ikke anderledes, end den kriminalitet som vi kender i forvejen. Der er for eksempel ingen forskel på, om der sker hærværk på en cykel eller hærværk på et informationssystem, idet der i begge tilfælde er tale om, at der sker ødelæggelse af en ting. Problemstillingen opstår, når det er den immaterielle data, som er lagret i systemet, som er angrebsobjektet.
Der opstår løbende nye situationer, hvor straffeloven ikke ud fra de eksisterende bestemmelser, tilstrækkeligt klart omfatter IT-kriminalitet, hvilket på grund af det strafferetlige legalitetsprincip, medfører en risiko for frifindelse, hvor der ellers ville have sket domfældelse. Dette var netop hvad der skete i sagen om Proms kemiske fabrikker, som senere bliver behandlet i specialet. I denne sag kunne gerningsbeskrivelsen om skriftlige erklæringer ikke anvendes analogt til at omfatte erklæringer indleveret på en diskette.

Lovgiver har på grund af den hastige udvikling, flere gange skulle vurdere straffelovens bestemmelser i forhold til IT-kriminalitet. I den forbindelse har lovgiver først skulle tage stilling til om IT-kriminalitet skulle beskyttes igennem de eksisterende bestemmelser, om der var behov for et særskilt kapitel, eller om der ligefrem var behov for en særskilt lov. I Danmark har man valgt at anvende de eksisterende bestemmelser så vidt det er muligt, og at tilpasse enkelte bestemmelser så gerningsindholdet også omfatter den nye teknologi. Hvor det har været nødvendigt, er enkelte ny bestemmelser opstået i forlængelse af de eksisterende. Lovgiver har dermed vurderet datarelate-

rede gerningsindhold i forhold til allerede kendte, nyopståede og fremtidige realistiske forbrydelser.

Med dette speciale vil hærværk af data blive analyseret, fordi data igennem en databehandling bliver omsat til beskyttelsesværdig information. Denne information kan lagres elektronisk i et informationssystem, eller ikke-elektronisk på et fysisk medie. I den nuværende lovgivning nyder data kun en direkte strafferetlig beskyttelse mod uberettiget adgang og anvendelse, for såvel fysisk og digitale data. Der er i straffeloven ikke en klar selvstændigt beskyttelse af denne data mod hærværk, men i stedet for nyder data en afledt beskyttelse af det bærende medie. Denne beskyttelse findes i hærværksbestemmelsen § 291, som beskytter en andens ting.

Dette speciale vil undersøge gældende rets beskyttelse af data, ved at analysere tingsbegrebet i hærværksbestemmelsen i forhold til data. Data er information, som kan ændres, slettes eller ødelægges. Spørgsmålet er så hvordan den uberettiget databehandling er strafbar efter § 291. Ting er som udgangspunkt løsøre og fast ejendom, men som afsnittet om gældende ret vil vise, så skal ting forstås meget bredt.

Analysen vil flere steder sammenligne dansk og norsk ret, fordi de gældende regler og principper overordnet er ens for begge lande. Norge har dog valgt at tilføje data som selvstændigt beskyttelsesobjekt i hærværksbestemmelsen, og det er derfor interessant af undersøge denne regulering, for dermed senere at vurdere om dansk ret skal afvente en videre fortolkning af tingsbegrebet, eller om der er behov for en lignende tilføjelse i dansk ret, for at sikre en tilstrækkelig beskyttelse af data.

Problemstillingen er på grund af informationsteknologien blevet mere relevant end tidligere, analysen med sker derfor som udgangspunkt ud fra IT-kriminalitet. Det er indenfor dette område, den afledte beskyttelse møder de største udfordringer. Det skyldes ikke kun samfundsudviklingen som har medført en større interesse for informationssikkerhed, med også fordi de tekniske lagringsløsninger går videre end de fysiske lagringsmuligheder giver mulighed for.

Der er ikke meget praksis på området om datahærværk, hvilket kan skyldes flere ting. Enten er det reelle problem ikke så stort, fordi den afledte beskyttelse er tilstrækkelig, eller også er bestemmelserne om informationskriminalitet ikke tilstrækkelig klart formuleret, så anklagemyndigheden med sikkerhed kan rejse tiltale efter et dækkende gerningsindhold.

Specialet vil i analysen fortolke det strafferetlige tingsbegreb, for at undersøge om data nyder en tilstrækkelig beskyttelse såfremt domstolen bliver stillet overfor en fortolkningsopgave.
Dernæst vil et forslag til en ny dansk bestemmelse blive præsenteret, som beskytter elektronisk lagret og ikke-elektronisk lagret data mod hærværk, for at vise muligheden for en tilstrækkelig klar lovhjemmel, som er et af straffelovens grundlæggende principper.

Formålet med analysens fortolkning af ting og det efterfølgende forslag til en ny bestemmelse, er at vurdere hvilken løsning der bedst sikrer en tilstrækkelig klar databeskyttelse mod hærværk, uden at gå på kompromis med det strafferetlige legalitetsprincip.

1.2 Problemformulering

Hvordan er data beskyttet mod hærværk og er denne beskyttelse tilstrækkelig?

1.3 Afgrænsning

Data er information, herunder programmer som fungerer i et edb-system. Information kan blandt andet være ophavsretlige værker, forretningshemmeligheder, kundekartoteker og retningslinjer. Behovet for et strafferetligt værn er forskellig, alt efter hvilken forbrydelse der er tale om. Dette speciale vil kun omhandle hærværk af data, og derfor afgrænse sig fra andre freds- og formuekrænkelsesforbrydelser, herunder blandt andet tyveri. Tyveri af data er lige så vigtigt at beskytte sig mod som hærværk, og efter gældende ret beskyttes kun erhvervshemmeligheder i markedsføringsloven, med enkelte tilføjelser i straffeloven. Denne afgrænsning skyldes den begrænsede plads, og den begrænsede tid, og det vil derfor ikke være muligt at gå tilstrækkeligt i dybden med datahærværk, hvis al informationskriminalitet skal behandles.

Når specialet sammenholdes med norsk ret, skyldes det at norsk ret, på trods af sammenlignelig strafferet og analyse af hærværksbestemmelsen, har valgt at tilføje data som selvstændigt beskyttelsesobjekt i hærværksbestemmelsen. Norge er det eneste nordiske land med denne løsning, idet både Sverige og Finland har valgt samme løsning som i Danmark, nemlig en fortolkning af eksisterende bestemmelser. Der vil ikke indgå norsk retspraksis i specialet. Problemstillingen omkring datahærværk er den samme i begge lande, og det er den norske løsning herpå, som er anderledes end den danske, der er interessant for specialet.

1.4 Metode

Specialet er opbygget således, at der først bliver redegjort for de grundlæggende principper og regler i strafferetten, som er relevant for dette speciale. Her vil reglen om klar lovhjemmel i straffelovens § 1 blive beskrevet, herunder mulighederne for fortolkning og analogi. Dette afsnit er vigtigt, da det både viser vigtigheden med en klar lovhjemmel, men også fordi afsnittet skal bruges i den senere analyse af hærværksbestemmelsen og den efterfølgende vurdering om en tilstrækkelig databeskyttelse mod hærværk.
I samme afsnit vil der blive redegjort for de internationale forpligtelser, som på grund af cybercrime-konventionens er bindendende for Danmark. Her vil konventionens definitioner og materielle regler, som er relevant for specialet om datahærværk blive præsenteret.
Ligeledes vil den norske strafferet blive præsenteret, idet den norske hærværksbestemmelse, løbende vil blive analyseret i forhold til den danske, for senere at give inspiration til et forslag om en lignende dansk lovregulering.

Jeg vil først anvende den retsdogmatiske metode, ved at analysere gældende ret *(de lege lata).* Jeg vil undersøge hvordan data beskyttes mod hærværk, ved at analysere forarbejderne til hærværks-

bestemmelsen. Jeg vil derudover analysere retspraksis på området, for at se hvordan domstolen anvender hærværksbestemmelsen i forhold til beskyttelsen af data. Jeg vil analysere tingsbegrebet, først i hærværksbestemmelsen, og senere tingsbegrebet i de andre formueretlige bestemmelser, i forbindelse med en fortolkning af hærværksbestemmelsen. Formålet er til sidst, at vurdere om data er tilstrækkeligt beskyttet som en ting.
I forbindelse med norsk ret, vil genstandsbegrebet blive analyseret i forhold til data, ud fra lovforarbejde og offentlige udredninger.
Analysen udarbejdes med udgangspunkt i IT-kriminalitet, fordi den teknologiske udvikling har sat fokus på databeskyttelse. Analysen vil dog inddrage ikke-elektronisk data også, og resultatet af analysen vil være et resultat at gældende ret for både elektronisk lagret og ikke-elektronisk lagret data.
Sidst i kapitlet om gældende ret, vil jeg analysere tilblivelsen af hackerbestemmelsen i § 263, stk. 2. Formålet er at anvende de bagvedlæggende hensyn i det efterfølgende kapitel om en selvstændig bestemmelse om beskyttelse af data mod hærværk.

Jeg vil lave et kapitel, som foreslår en ny hærværksbestemmelse som selvstændigt beskytter både elektronisk lagret og ikke-elektronisk lagret data *(de lege ferenda)*. Denne bestemmelse skal supplere den eksisterende hærværksbestemmelse.
I kapitlet vil først den norske lovændring blive analyseret, for dernæst at give et bud på hvordan dansk lovgivningen bør udformes. Den nye bestemmelse bliver i den forbindelse analyseret, for at sikre en tilstrækkelig beskyttelse af data, med respekt for legalitetsprincippet.

Jeg vil starte hvert afsnit med en indledning med afsnittets formål. Sidst i hvert afsnit vil jeg lave en del-konklusion, som skal samle op på afsnittet. Formålet er at danne en rød tråd gennem specialet, og på den måde at give læseren et godt overblik.

De væsentligste kilder i specialet er betænkning nr. 1485 fra 2006 og betænkning nr. 1417 fra 2002. Disse betænkninger har begge analyseret og vurderet straffelovens eksisterende bestemmelser, herunder hærværksbestemmelsen, i forhold til IT-kriminalitet. I begge betænkninger er man kommet frem til, at data nyder en afledt beskyttelse af det bærende medie, som ikke har givet behov for en tidligere lovændring. Derudover anvendes både den danske og den norske straffelov, som holdes op mod hinanden i forhold til datahærværk. I forbindelse med norsk ret, vil også udredning nr. 2 fra 2007 være en væsentlig retskilde, da den danner grundlag for tilføjelsen af data i den norske hærværksbestemmelse.

I samarbejde med anklagemyndigheden i Aalborg, vil jeg undersøge hvordan praktikere ser på problemstillingen omkring datahærværk. På den måde får jeg en fornemmelse af hvorvidt der reelt er et problem, eller om det endnu kun er et teoretisk problem. Anklagemyndigheden vil fungere som sparingspartner, såfremt jeg støder på teoretiske problemstillinger, som jeg ikke kan finde prøvet i praksis. Derudover vil anklagemyndigheden bidrage med eventuelle sager, som relatere sig til problemformuleringen, for dermed at bidrage med praktiske problemstillinger til den teoretiske analyse.

2. DET REDEGØRENDE KAPITEL

2.1 Indledning

Dette kapitel omhandler de grundlæggende principper og regler, som er relevante for specialet. Først vil straffelovens legalitetsprincip blive præsenteret. Legalitetsprincippet skaber fundamentet for specialet, idet fortolkning af tingsbegrebet i hærværksbestemmelsen er afgørende for om data er tilstrækkeligt beskyttet mod hærværk.
Dernæst vil de internationale forpligtelser som er relevant for specialet blive redegjort for. Det er i denne forbindelse Cybercrime-konventionen, som indeholder definitioner og materielle regler, som skal respekteres af dansk ret. Når der senere vurderes om dansk ret tilstrækkeligt beskytter data mod hærværk, skal vurderingen også tage højde for den internationale forpligtigelse.
Efterfølgende redegøres der for den norske straffelov. Den norske hærværksbestemmelse er senere i analysen også relevant at se på, da norsk ret, på trods af lignende straffelov og principper, har valgt en anden løsning på datahærværk, end den danske. Den norske løsning inspirerer til den dansk lovændring, som senere i specielt bliver præsenteret.
Formålet med dette kapitel er at danne et fundament for den efterfølgende analyse og vurdering.

2.2 Det strafferetlige legalitetsprincip

De nationale regler for straf findes hovedsageligt i straffeloven. Straffeloven suppleres af særlove som for eksempel selskabsloven eller ophavsretsloven, der også indeholder straffebestemmelser.
Straffeloven er delt i en almindelig del og en speciel del. Den almindelige del indeholder grundlæggende regler, som gælder for hele straffeloven, mens den specielle del indeholder de bestemmelser, som beskriver de strafbare handlinger.
I dette afsnit vil legalitetsprincippet blive præsenteret, sammen med fortolknings- og analogireglerne for princippet.

2.2.1 Legalitetsprincippet

IT-kriminalitet er som nævnt ikke anderledes end den almindelige kriminalitet. Det særlige ved IT-kriminalitet er ikke fremgangsmåden men redskabet, idet der ved berigelseskriminalitet anvendes et andet redskab end tidligere. Der er for eksempel ikke forskel på, om der sker bedrageri mellem en køber og en sælger på gaden, eller om det sker via mail. Sker der en uberettiget formueforskydning, som skyldes den disposition, som gerningsmanden foretog, da er gerningsindholdet for bedrageri opfyldt.[1] Der er dog sammen med den teknologiske udvikling opstået nye typer af forbrydelser, og derfor er der løbende tilføjet nye bestemmelser i strafferetten og ændret ordlyden i andre.
Når der opstår en situation, som ønskes kriminaliseret, er opgaven at beskrive et gerningsindhold. Gerningsindholdet skal være så bredt at flere næsten ens situationer passer ind. Det sker blandt

[1] Kommenteret straffelov – specielle del, side 536-539

andet ved at give bestemmelserne et åbent ordvalg. Gerningsindholdet skal dog omvendt være så konkret, at legalitetsprincippet er opfyldt, jf. straffelovens § 1 og EMRK art. 7, stk. 1.

Det strenge lovhjemmelskrav i straffelovens §1 skyldes blandt andet at det skal være forudsigeligt hvad der er lovligt og hvad der er strafbart. Lovhjemmelskravet betyder, at der skal være hjemmel til staf enten direkte i straffeloven, i en særlov, eller i en bekendtgørelse, som er udfærdiget med hjemmel i lov.
Hvis en straffebestemmelse tidligere har været gældende, men bliver ophævet, da er der sket en afkriminalisering. I sådan et tilfælde kan der ikke senere dømmes, uanset årsagen til afkriminaliseringen. Det gælder også, hvis lovgiver ved en fejl har afkriminaliseret, uden at havde taget højde for en senere konkret problemstilling. Det eneste der er undskyldeligt er typografiske fejl, hvilket kom til udtryk i U2011.877V. I denne sag havde en tysker fanget rejer inden for den danske basislinje. Dette var ulovligt efter den oprindelige lovgivning, men på grund af en typografisk fejl, var det lovligt efter den nye lovgivning. Tyskeren blev dømt, blandt andet fordi han var klar over at der var tale om en fejl og derfor ikke kunne havde misforstået reglen.

Hvis en handling er uønsket i et samfund, men ikke gjort strafbar ved lov, da skal der ske frifindelse. Lovgiver må så efterfølgende tilpasse loven, således den uønskede handling bliver gjort strafbar. Der er efter dansk ret, som udgangspunkt ikke noget i vejen for at lave straffebestemmelser med tilbagevirkende kraft, men idet vi har inkorporeret EMRK, vil det være i strid med dennes artikel 7 at gøre det, samt betænkeligt i et retssamfund hvor borgeren skal vide sig sikker på sin ret.
Ligesom andre danske love skal respektere internationale konventioner som Danmark har tiltrådt, skal straffeloven også respektere EMRK.
Derudover skal danske lovregler fortolkes til fordel for den almindelige EU ret. Denne fortolkningsregel gælder dog for Danmarks vedkommende kun for de EU-regler, som er bindende for Danmark, på grund af Danmarks retlige forbehold. Danske lovregler må altså ikke hindre den frie bevægelighed, hvilket blandt andet skete i dommen U.2011.539H. I dommen blev de tiltalte frifundet for at sejle på vandscootere i danske farvande. Det var ikke lovligt at sejle på vandscootere i Danmark, men da sådan en bestemmelse begrænser det frie marked, betød EU-reglerne at de tiltalte ikke kunne straffes.[2]

2.2.2 Fortolkning

Når der i en bestemmelse er beskrevet et gerningsindhold, som ønskes kriminaliseret, er spørgsmålet hvordan bestemmelsen skal fortolkes, når den ikke er tilstrækkelig klar. Det kan enten være på grund af forkerte og for dårlige ordvalg fra lovgivers side, eller på grund af en uforudset udvikling i samfundet. En uforudset udvikling kan være den teknologiske udvikling, der netop er interessant for dette speciale.

[2] Kommenteret straffelov – almindelige del, side 117-122

Fortolkning i strafferetten sker som udgangspunkt ligesom al anden lovfortolkning. Der er ikke et princip om at anvende den for tiltalte mest gunstige fortolkning, som det er gældende i bevisretten, hvor tvivlen om tilstrækkelig bevis skal komme den tiltale til gode *(in dubio pre reo).*
Straffebestemmelser skal som udgangspunkt fortolkes ud fra lovtekstens sproglige udtryk, og hvis der er tvivl om hvor langt ordene kan strækkes, har domstolen vist sig at være tilbageholdende med at lægge mere i ordene, end det med sikkerhed kan forudsættes, er ordenes betydning.
Hvis lovteksten kan have flere forståelser, må domstolen vende sig mod bestemmelsens formål og motiver, for at finde frem til ordlydens forståelse. Der er ingen regel om hvornår der skal ske en indskrænkende eller udvidende fortolkning, men den indskrænkende fortolkning har haft en stor plads i strafferetten. Det kan blandt andet ses, når den tiltalte frifindes, på trods af en naturlig sproglig forståelse af ordlyden, burde føre til domfældelse. I U.1963.1029V blev en 16-årig frifundet for brugstyveri, da han i spirituspåvirket tilstand, brugte sin fars bil til at køre en kammerat hjem. Retten mente ikke, at det kunne antages, at dette forhold havde været tilsigtet at gøre strafbart som brugstyveri, og der forelå derfor materiel atypicitet.
Nogen gange sker der en udvidet fortolkning. Det ses blandt andet når en undladelse dømmes ligesom en handlingsforbrydelse. I dommen U.1984.645V tabte den tiltalte en cigaret på et tæppe under et indbrud. Da han undlod at handle, ved for eksempel at slukke cigaretten, blev han dømt for at forvolde ildebrand, jf. straffelovens § 181.

Når et forhold fremtræder på en anden måde end beskrevet i straffebestemmelsen, men dog alligevel dækker over beskrivelsen, kan der bruges en udvidet fortolkning eller en analogislutning. Det betænkelige med den udvidet fortolkning eller analogislutning, er at en overfortolkning kan medføre, at en tiltalt bliver dømt for et forhold, der ikke er tilstrækkeligt klart hjemlet. Fortolkning og analogislutning må aldrig gå ud over hjemmelskravet.
I modsætning til civilretten, hvor der er en part på begge sider, der har personlig interesse i fortolkningen, og dermed i dommens udfald, er konsekvensen af en begrænset strafferetlig fortolkning *kun* en frifindelse. Frifindelsen kan så medføre en lovændring, for at sikre at en fremtidig lignende situationer fører til straf.[3] Dette var tilfældet i sagen om Proms Kemiske fabriker, som vil blive gennemgået i næste afsnit om analogi.

Praktisk sker fortolkningen i flere faser. Først ser domstolen på ordlyden, som er det klare udgangspunkt ved enhver lovfortolkning. Såfremt ordlyden ikke er tilstrækkelig klar i den enkelte bestemmelse, må domstolen se på hvordan den samme ordlyd fortolkes i andre bestemmelser i samme lov. I mange tilfælde er der ikke en ordforklaring i loven, og derfor er hovedreglen at ordende har den betydning, som er almen kendt. Ordene har derfor som udgangspunkt samme betydning i straffeloven som i andre love. I en fortolkningsproces, som går udover en ordlydsfortolkning, skal resultatet hele tiden tage bestemmelsens ordlyd i betragtning, således fortolkningen i sidste hele drejer sig om ordlyden.

[3] Kommenteret straffelov – almindelige del, side 123-128

Hvis ordlyden stadig ikke er tilstrækkelig klar, må domstolen som nævnt, se på bestemmelsens formål. Er der tale om en særlov som for eksempel arbejdsmiljøloven, kan lovens overordnede formål, et sikkert og sundt arbejdsmiljø, hjælpe til bestemmelsens betydning. Straffeloven har ikke et overordnet formål, men er derimod inddelt i kapitler, som så kan hjælpe til en fortolkning af bestemmelsen.
Det næste skridt til en korrekt fortolkning kan være strafferammen. Hvis der er tale om en mild strafferamme, kan det tale for en bred fortolkning af bestemmelsen, hvorimod en streng strafferamme kan tale for en indskrænkende fortolkning. Denne fortolkningsfase er dog begrænset, fordi blandt andet særlove ofte har en strafferamme som rummer bøde, lige såvel som juridiske personer kun kan idømmes bøde. Sidste fase er en limitationsfortolkning. Det betyder, at en bestemmelse formodes kun at kunne strækkes så langt, at nabobestemmelserne ikke overlappes. På den måde afgrænses bestemmelserne til et selvstændigt område. Denne fortolkningsmetode blev anvendt i aids-dommen, U.1994.520/2h. I denne dom havde den tiltale haft ubeskyttet samleje med 23 kvinder, uden først at oplyse dem om at han havde aids. Manden blev tiltalt for § 252, stk. 1, om at havde forvoldt nærliggende fare for nogens liv. § 252, stk. 1 blev fortolket i forhold til en tidligere § 256, om smittespredning af kønssygdomme. Fordi § 256 var blevet ophævet, og der i den forbindelse ikke var sket ændringer af § 252, skete der en limitationsfortolkning, der gjorde at forholdet ikke kunne dømmes efter § 252. § 252 skulle altså respektere området, som var dækket af § 256.[4]

2.2.3 Analogi

Der er en næsten usynlig grænse mellem en vid fortolkning og en analogislutning. Da § 1 indeholder ordende "ganske må ligestilles med" er der hjemmel til en vis analogislutning, men denne hjemmel må dog være noget begrænset, idet EMRK art. 7 ikke har denne formulering.
En analogislutning til skade for en tiltalt er dog ikke helt afvisende, når bare nogle enkelte betingelser er opfyldt. For det første kræves det, at der findes en straffebestemmelse at tage udgangspunkt i. Dernæst skal det aktuelle forhold kunne ligestilles med den eksisterende straffebestemmelse så åbenbart, at en frifindelse vil virke som ren formalisme.[5]
Domstolen accepterede en udvidet fortolkning i U.1996.356Ø som handlede om kædebreve. Tiltalte havde været med i et system hvor disketter fungerede på samme måde som kædebreve. Man kunne mod betaling på 50 kr. modtage en kode, som aktiverede et program. Programmet kopierede derefter sig selv, og denne kopi blev sendt videre til næste led i kæden. Denne skulle så også betale 50 kr. for at få en kode, og således fortsatte kæden. Formålet var, at de mange betalinger skulle generere et profit. Landsretten fandt at systemet var bygget op ligesom et kædebrevsystem, med samme formål, nemlig en økonomisk gevinst, og derfor var det aktuelle forhold strafbart.

[4] Det strafferetlige legalitetsprincip, side 283 - 294
[5] Kommenteret straffelov - almindelige del, side 129-130

Derimod accepterede domstolen ikke en udvidet fortolkning i øster landsretsdommen af 13/2 1995 om Proms kemiske fabrikker. Her havde virksomheden givet urigtige oplysninger på diskette, som ikke var ikke omfattet af den daværende § 163, eller dennes analogi om urigtige skriftlige erklæringer. Dette skyldtes, at på trods af formålet med bestemmelsen, så havde det aktuelle forhold været drøftet i forarbejderne til 1985-ændringen. En analogislutning kræver, som netop anført, at det skal kunne anses som en tilfældighed eller ikke stemmende overens med lovgivers vilje, at forholdet ikke er omfattet af straffebestemmelsen. [6]
I udarbejdelsen af betænkning nr. 1032 fra 1985, var man klar over at denne risiko forelå, men mente ikke at der på det pågældende tidspunkt var behov for en lovændring.

2.3 Cybercrime-konventionen

Den internationale Cybercrime-konvention er den første konvention om bekæmpelse af internet- og netværksbaseret kriminalitet. Formålet med konventionen er at sikre ensartet lovgivning til bekæmpelse af IT-kriminalitet, og på den måde styrke den internationale samarbejde. Konventionen blev vedtaget i 2001 og trådte i kraft den 1. Juli 2004. Danmark tiltrådte konventionen den 1. oktober 2005, efter at have tilpasset den danske lovgivning til konventionen ved betænkning nr. 1417 fra 2002 om IT-kriminalitet.[7]

Konventionen er opdelt i fire kapitler, med overskrifterne, ”anvendelse af definitioner”, ”foranstaltninger på nationalt plan”, ”internationalt samarbejde”, og ”afsluttende bestemmelser”.
Det første kapitel definerer ”edb-systemer”, ”elektroniske data”, ”serviceudbyder” og ”trafikdata”, kapitel 2 handler om den materielle strafferet, processuelle bestemmelser og regler om jurisdiktion. Kapitel 3 handler om det internationale samarbejde og gensidig retshjælp.

2.3.1 Definitioner

Cybercrime-konventionens definitioner er vigtige, fordi den nationale lovgivning skal respektere cybercrime-konventionen. Som netop skrevet i afsnittet om fortolkning, er udgangspunktet en ordlydsfortolkning, og såfremt domstolen skal fortolke sine bestemmelser i forbindelse med IT-kriminalitet, kan domstolen se på cybercrime-konventionens definitioner i forbindelse med de nationale bestemmelsers formål og bagvedliggende hensyn. Når konventionen sikrer ensartet fortolkning blandt alle de deltagende lande, sikres det at grænseoverskridende kriminalitet behandles ens. Det er især vigtigt indenfor cybercrime med denne ensartethed, idet grænserne er mere flydende i cyberspace.
De vigtigste definitioner for dette speciale er definitionen af et edb-system og af data.

Et edb-system defineres i konventionens artikel 1, litra a;

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

[6] IT-retten side 724-725
[7] TfK.2013.240, pkt. 3.1.2

Data defineres i konventionens artikel 1, litra b;

> *"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"*

Formålet med at have definitionerne med her, er at specialet vil analysere gældende ret, samt diskutere om gældende ret er tilstrækkelig. Når data skal vurderes i forhold til ting i hærværksbestemmelsen, er det med udgangspunkt i cybercrime-konventionens definition.

2.3.2 Materielle regler

De materielle regler kommer til udtryk i konventionens artikel 2-13, hvor artikel 4 og 5 er særligt relevante for dette speciale. Som skrevet ovenfor, er de danske regler om IT-kriminalitet tilpasset af konventionens materielle regler, og konventionens ordlyd må derfor hjælpe i en eventuel uklarhed om de nationale bestemmelsers anvendelsesområde.

Indgreb i data beskrives i konventionens artikel 4;

> *"1. 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.*
>
> *2. En part kan forbeholde sig ret til at kræve, at den i stk. 1 angivne handling har forvoldt betydelig skade."*

Indgreb i systemer beskrives i konventionens artikel 5;

> *"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."*

Som det kommer til udtryk, er der en særskilt beskyttelse af data og en særskilt beskyttelse af edb-systemer i konventionens artikel 4 og 5. De to bestemmelser skal senere i specialet hjælpe til, at vurdere om data nyder en tilstrækkelig beskyttelse, eller om der er behov for yderligere regulering af national ret, for at leve op til de nationale forpligtelser overfor cybercrime-konventionen.

2.4 Norsk strafferet

Det er interessant at se på den norske hærkværksbestemmelse i forhold til den danske. Det er det fordi straffeloven i Danmark og i Norge, på mange måder er sammenlignelige. Der er også indenfor økonomisk kriminalitet en sammenlignelighed både i bestemmelsernes ordlyd, men også i hensynene bag bestemmelserne. Dette vil komme til udtryk her, når den norske hærværksbestemmelse analyseres sammen med den danske.

Den norske straffelov er fra 1902, og den er inddelt i tre dele. Den første del svarer til den danske straffelovs almindelige del, og indeholder blandt andet definitioner og strafferetlig virkning. Anden og tredje del minder om den danske specielle del. Anden del indeholder forskellige forbrydelser, mens tredje del indeholder forskellige forbrydelser, som er mindre alvorlige.
Straffeloven forventes at blive erstattet med en ny straffelov fra 2005, som er vedtaget, men er ikke endeligt trådt i kraft endnu. Flere af bestemmelserne som er vedtaget, er inkorporeret i 1902-straffeloven, indtil den endelige 2005-straffelov træder i kræft. Det vides endnu ikke hvornår den nye straffelov endeligt træder i kræft, men det var tidlist bestemt til 2014, idet politidirektøren mente at straffeloven skulle lægges ind i politiets edb-system før ikrafttrædelsen. Den endelige 2005-straffelov er endnu ikke trådt i kræft.[8]

I forhold til IT-kriminalitet tilpassede Norge i første omgang, ligesom i Danmark, de eksisterende bestemmelser med IT-kriminalitet. Det skete i forbindelse med revision af straffeloven i 1985. Norge kom i den forbindelse frem til samme resultat som Danmark, nemlig at data havde en afledt beskyttelse af det bærende medie.[9]

Ligesom der i Danmark, har været nedsat udvalg til at vurdere de danske bestemmelse i forhold til IT-kriminalitet og i forhold til cybercrime-konventionen, har Norge også nedsat udvalg. Norge har også tilsluttet sig cybercrime-konventionen, og har derfor haft samme behov for at gå sine straffebestemmelser efter i forhold til IT-kriminalitet, heriblandt også hærværksbestemmelsen, som indtil 2004, havde samme indhold som den danske. Denne lovændring bliver gennemgået i det senere kapitel om en selvstændig beskyttelse.

2.5 Sammenfatning

I dette kapitel er der redegjort for det strafferetlige legalitetsprincip, som har til formål at sikre en klar retsstilling i retssamfundet. Legalitetsprincippet stiller krav om at straffebestemmelser skal udformes så bredt, at flere lignende situation er omfattet af den samme beskrivelse, men dog ikke bredere end at det klart fremgår af bestemmelsen, hvad der er strafbart. Gerningsbeskrivelsen kan være udformet af vage ordvalg, eller der kan have sket udvikling i samfundet, som gør det uklart hvordan eller hvorvidt en handling er omfattet af gerningsbeskrivelsen. I sådan en situation må straffebestemmelsen fortolkes, ud fra en ordlyds-, formåls, straf- og limitationsfortolkning. I nogle tilfælde kan handlingen minde om en eksisterende bestemmelse som dog ikke er dækket klart af ordlyden. Hvis det vil være ren formalisme at frikende, kan denne handling straffes ud fra en analogifortolkning. Denne fortolkning er dog betænkelig, idet den europæiske menneskeretskonvention ikke giver udtryk for denne fortolkningsmulighed.

[8] https://lovdata.no/dokument/NL/lov/2005-05-20-28, 1. maj 2015, kl. 20.00
[9] NOU nr. 31 fra 1985, pkt. 4.3.4

I kapitlet er, den for specialet relevante del af cybercrime-konventionen også blevet gennemgået. Denne konvention har til formål at sikre en ensartet lovgivning til bekæmpelse af IT-kriminalitet, og da Danmark har tiltrådt denne, skal nationale definitioner og materielle regler respektere konventionen.
Endeligt er den norske strafferet blevet præsenteret, da norsk ret som den eneste af de nordiske lande, har tilføjet en selvstændig beskyttelse af data i sin hærværksbestemmelse. Norsk ret er her blevet præsenteret, fordi den følgende analyse løbende vil inddrage det norske lovforarbejde vedrørende datahærværk.

4. GÆLDENDE RET (de lege lata)

4.1 Indledning

Dette kapitel handler om den gældende retstilling for hærværk af data.
Først vil der komme et afsnit, som redegør for, hvad data egentlig er. I den forbindelse vil også information og viden blive beskrevet, idet information og viden opstår af data, der er behandlet. I dette afsnit bliver det også gjort gældende, hvorfor der overhovedet er et behov for databeskyttelse, for således at danne et indtryk af vigtigheden med analysen.
Inden analysen går i dybden med hærværk af data, kommer der et afsnit, som beskriver den overordnede datakriminalitet, for at give et overblik over gældende retsbeskyttelse af data og information. I dette afsnit kommer det også til udtryk, at det særligt er datasystemet og ikke data der nyder beskyttelse mod angreb, mens data nyder en bredere beskyttelse mod uberettiget adgang om uberettiget anvendelse.
I afsnittet om gældende ret analyseret hærværksbestemmelsen, der som udgangspunkt er det strafferetlige værn mod datahærværk. Hærværksbestemmelsen beskytter en andens ting, og derfor vil analysen gå i dybden med at finde ud af, hvad tingsbegrebet dækker over. Igennem forarbejder, betænkninger og retspraksis vil det komme til udtryk at data har en afledt beskyttelse af det bærende medie.
Den afledte beskyttelse for elektronisk lagret data, er siden sidste betænkning kommet ud for nye udfordringer på baggrund af den teknologiske udvikling. Disse udfordringer bliver undersøgt for senere at kunne vurdere om databeskyttelsen er tilstrækkelig. Derudover er der i cybercrimekonventionen et krav om at data nyder en selvstændig beskyttelse mod hærværk, og denne problemstilling bliver også belyst.
På baggrund af gældende rets uklare beskyttelse, som også møder nye udfordringer, undersøges dernæst muligheden for at fortolke tingsbegrebet udvidende, til at omfatte data som et selvstændigt beskyttelsesobjekt. Denne fortolkning sker på baggrund af de principper, der blev redegjort for i sidste kapitel, og i den forbindelse analyseres tingsbegrebet generelt for hele straffeloven.
Som et sidste afsnit, vender analysen sig mod en tidligere lovændring på baggrund af en uklar bestemmelse, som dog også havde rum for fortolkning. Det er hackerbestemmelsen i § 263, stk. 2, som har haft samme problemstilling, som data har i forhold til hærværk. Formålet med afsnittet er at stille spørgsmålstegn ved om en udvidet fortolkning er den rette vej at gå, for at sikre en klar retsstilling, som er i overensstemmelse med det strafferetlige legalitetsprincip.

4.2 Data

I dette afsnit vil data blive beskrevet, og i den forbindelse hvordan information og viden en naturlig følge heraf.
Ud over en redegørelse af data, vil beskyttelsesbehovet for data også blive gennemgået, for således at give udtryk for, hvorfor databeskyttelse mod hærværk er vigtigt.

4.2.1 Data, information og viden

Data er oplysninger, som skal behandles for at blive til information. Informationer kan tilegnes og dermed give viden.

Data optræder i tre datatyper som enten er heltal, flydende tal eller tegn. Disse data kan behandles enkeltvis eller i kombination med hinanden, hvilket kaldes datastruktur, men er kun anvendelige, hvis brugeren kender meningen med talkombinationen. Det er præsentationen af data, som bestemmer betydningen af dataen.

Et eksempel på data kan være en talkombination som 130825. Hvis man ved, disse tal er en fødselsdato, altså den 13. August 1925, da er dataen omsat til brugbar information. Talkombination kan også betyde andet end en fødselsdato, det kan være resultatet af en optælling. Informationen vil således være 130.825 stk.

Når dataen lagres, sker det i et system, som giver dataen mening. Det kan for eksempel være telefonnumre en telefonbog eller kundeoplysninger i et kundekartotek. På baggrund af den udvikling der er indenfor informationsteknologi, kan data også lagres digitalt, men det grundlæggende er stadig, at data kun er tal eller tegn.

I et informationssystem kaldes præsentationen også for dataformatet, som er det format, systemet arbejder ud fra. Det er dataformatet, der bestemmer hvordan dataen skal give betydning, og det er dermed forskellen på to dataformater, der er skyld i at den samme data, kan resultere i to forskelligere informationer. Når data overføres fra et system til et andet, da skal begge systemer have samme dataformat, for at gengive samme information. Har modtageren ikke samme format som afsender, vil modtager ikke kunne forstå den modtaget information.[10]

På baggrund af en behandlingen af data opstår information, som ligger mellem data og viden. Viden er den videnskabelige erkendelse som opstår, når informationen tilegnes. Viden adskiller sig således fra at tro på baggrund af meninger, fordi viden er en sandhed som er opstået på baggrund af den indsigt man får igennem sandfærdige informationer.[11]

Når data behandles elektronisk, kan den optræde i tre faser, nemlig inddata, lagret data og uddata. Derudover kan data transmitteres mellem flere systemer.

Når data er i første fase som inddata, kan data for eksempel være et spørgeskema. Spørgeskemaet kan være besvaret med ja eller nej, hvilket så er data.

Når dataen er lagret, optræder dataen i sin anden fase, og hvordan dataen lagres er uden betydning. Det kan ske i et register, et datasystem eller på et andet databærende medie.

Den sidste fase er uddata, som er en betegnelse for de informationer, som dataen giver efter en behandling i datasystemet.

[10] http://www.denstoredanske.dk/It,_teknik_og_naturvidenskab/Informatik/Software,_programmering,_internet_og_webkommunikation/data

[11] http://www.denstoredanske.dk/Sprog,_religion_og_filosofi/Filosofi/Filosofiske_begreber_og_fagudtryk/viden

Når elektronisk data transmitteres, kan det ske på flere måder. Data kan sendes som almindelig post, lagret på et bærende medie. På denne måde optræder dataen dog stadig som i den anden fase som lagret data. Data kan også transmitteres via internettet.
Data har i alle faserne behov for strafferetlig beskyttelse, fordi dataen i alle faser kan blive udsat for hærværk. Det strafferetlige værn mod dette vil blive behandlet løbende i de næste afsnit.[12]

4.2.3 Beskyttelsesbehovet

Som netop skrevet, giver data i form af information, en viden til den, der tilegner sig den. Denne viden forudsætter at informationen ikke er usand, som kan skyldes at dataen er forkert, eller at dataen har været udsat for hærværk.
Information spiller en vigtig rolle i samfundet, blandt andet fordi beslutninger som påvirker vores hverdag, træffes på baggrund af informationerne, i form af viden og erfaringer. De beslutninger vi træffer kan i sig selv være viden, i form af det talte sprog, og således opstår information på baggrund af tidligere information.
Indenfor den digitale verden af information, har den teknologiske udvikling givet mulighed for endnu bredere informationsspredning. Denne udvikling har påvirket samfundet fra et almindeligt industrisamfund til et samfund af informationsindustri. Dermed er det ikke informationen i sig selv der er noget nyt, men derimod anvendelsesmulighederne for information. De nye anvendelsesmuligheder kan være meget omkostningsfulde. Derfor bliver informationen et formuegode, som der forhandles og investeres i. Problemet med denne udvikling er at informationer ikke er en fysisk ting, som andre formuegoder, men er derimod et immaterielt formuegode, som kun delvis kan behandles efter de almindelige formueretlige- og strafferetlige regler.[13]

Erhvervshemmeligheder eller data fra en legal dataindsamling om forbrugere eller konkurrerende virksomheder, er blot to eksempler på informationer som kræver et strafferetligt værn. Mulighederne er mange, og jo flere måder data kan behandles og dermed give brugbar information, jo større er behovet for en beskyttelse heraf.
Beskyttelsesinteressen for data er stor, fordi især virksomheder er meget afhængig af denne data. Når virksomheden lagrer data, har de en tillid til at denne data er korrekt og beskyttet mod angreb og uberettiget anvendelse. Erhvervshemmeligheder, er informationer som er baggrunden for virksomhedernes eksistens. Hvis disse hemmeligheder stjæles eller ødelægges, kan virksomheden risikere at skulle tvinges til at lukke.[14]

Behovet for at beskytte informationer mod angreb er ikke kun mod udefrakommende. I nogle situationer kan det være en person med en berettiget adgang, der ændrer eller på anden måde ødelægger disse data. Det kan for eksempel være salgschefen der bliver fyret, og derfor frygtes at slette kundekartoteket, eller det kan være forretningshemmeligheder, der er lagret digitalt, som på grund af en medarbejder bliver skadet eller går tabt. Det kan også være en person, som tilføjer

[12] EDB-strafferet, side 44-60
[13] IT-retten, side 71-74
[14] Erhvervsspionage, side 82-84

en logisk bombe, med det eneste formål, at slette lageret for information efter en periode. Disse ødelæggelser har ikke kun en fiktiv værdi, men også en økonomisk værdi. Denne værdi kommer til udtryk når informationerne udsættes for angreb, som medfører et behov for reetablering af tabte data, og når informationerne handles.

I dommen 1987.216Ø som omhandlede elektronisk lagret data, blev tabet opgjort til 100.000 kr. til ekstern bistand og interne mandetimer til reetablering af den tabte data og efterfølgende vedligeholdelse. I en anden dom om elektronisk lagret data, SH2003.P-0012-00 havde en medarbejder i forbindelse med sin fyring, ændret kodeordet til virksomhedens bogføringsfil og slettet noget data. I denne sag blev der rejst et krav på 234.062,53 kr. til dækning af den eksterne bistand til reetablering. Kravet blev nedsat på grund at de forbedringer der fulgte med reetableringen, men tabet blev samlet opgjort til 180.000 kr.

Ud over den omkostning der er i reetablering af tabte data, har den egentlige information som nævnt også en økonomisk værdi. Er der for eksempel tale om et ophavsretligt værk, er der tale om en information, som er omfattet af formueretten. Det betyder at værket kan omsættes og anvendes med respekt for den der har den ideelle rettighed. Den der har den ideelle rettighed over et værk, nyder en beskyttelse mod at andre gør værket tilgængelig for almenheden og mod at værket spredes.
Når rettighedshaveren over et program, et register med behandlet data eller et andet ophavsretligt værk, sælger værket til for eksempel en virksomhed, er der sket konsumption. Konsumption betyder at ejendomsretten er overgået til en anden, som så kan gøre videresælge værket på det frie marked. Dermed er behandlede informationer et formuegode, som har en økonomisk værdi. Dette immaterielle formuegode har samme behov for en strafferetlig beskyttelse som materielle formuegoder har imod blandt andet hærværk[15]

Meget aktuelt er virksomheder, der tjener penge på at indsamle oplysninger om vores færden på internettet. Denne dataindsamling sker helt lovligt ved hjælp af cookies, som accepteres af brugerne på internettet. Disse data samles og sælges som information til andre virksomheder, der kan bruge denne information i forbindelse med sin markedsføring.[16]

4.3 Datakriminalitet

I dette afsnit ses der på informationskrænkelserne generelt, idet flere situationer straffes allerede ved den uberettigede adgang eller ved den efterfølgende anvendelse af informationerne.
Overordnet set er der fire kategorier for informationskrænkelser, nemlig angreb, adgang, anvendelse og videregivelse. Disse fire kategorier kan opdeles i elektronisk lagret information og ikke-elektronisk lagret information.

[15] IT-retten, side 564-566
[16] http://www.dr.dk/Nyheder/Penge/2014/08/26/171526.htm , 6. Maj 2015, kl. 15.00

4.3.1 Angreb på systemet

Angreb kan beskrives som den yderste beskyttelse mod en udefrakommende. De fysiske angreb kan være ødelæggelse, beskadigelse eller bortskaffelse af systemet, mens angrebene mod edb-systemet i høj grad drejer sig om at belaste brugen heraf.
Er der tale om et edb-system kan systemet ud over de fysiske angreb blive udsat for Malware og Denial-of-Servise, som er de mest kendte former for IT-angreb.
Malware er et begreb, som dækker over virus, orme, trojanske heste og andre ondsindede programmer. Det som de alle har tilfældes, er at de laver skade på systemet og programmerne. Nogle sletter indholdet af harddisken, mens andre gør brug af computerens hukommelse til at fremvise reklamer. De uønskede programmer kan have alverdens funktioner, men samlet set fungere de uden brugerens ønske eller opmærksomhed. For at aktivere et malware-program, kan brugeren havde trykket på et link i en mail, set en video på facebook eller åbnet et ukendt program.
DoS er en form for hærværk, som hindrer en bruger i almindeligt brug af sit system. Det sker ved at systemet bliver overbelastet, ved eksempelvis at modtage store Internet Protokol-pakker, således internettet ikke kan sende og modtage andet.
Det afgørende for angreb er, at systemet ikke fungerer efter hensigten.

De tre bestemmelser i straffeloven som beskytter systemet mod angreb er § 193 om omfattende forstyrrelser i driften, § 293 om brugstyveri og § 291 om hærværk.[17]

4.3.2 Adgang til informationer

Adgang beskriver den situation hvor nogen kommer ind i et system, som denne ikke har en berettiget adgang til. Det kan være en uberettiget indtrængen i de private gemmer, eller det kan være en, der skaffer sig adgang til et system, som tilkommer en anden at have adgang til.
Den beskyttelse der ydes mod uberettiget adgang til informationer, findes for ikke-elektronisk lagret information i § 263, stk. 1, og for elektronisk lagret information i den almindelige hackerbestemmelse, § 263, stk. 2. Derudover beskyttes lukkede systemer og kommercielle systemer efter henholdsvis § 263a og § 301a.

4.3.3 Anvendelse af informationer

Anvendelsen er nok den mest krænkende kategori af de tre mulige. Her er gerningsmand kommet ind i systemet, har gjort sig bekendt med indholdet, og anvender så denne information.
Det kan for eksempel være identitetstyveri, hvor gerningsmanden udgiver sig for at være en anden, for så at købe noget, der giver gerningsmanden en berigelse og offeret et lignende tab.
Identitetstyveri er som sådan ikke strafbart efter dansk ret, men det er det efter norsk ret.
Der kan også være tale om at anvende eller offentligøre forretningshemmeligheder. Ved at offentliggøre et selskabs forretningshemmelighed, lider selskabet et tab.
Phissing-mails er en anden type for anvendelse, hvor offeret modtager en mail, som ser ud til at være af en anden afsender. Eksempelvis kan mailen fremstå som om den er fra SKAT, med ønske

[17] Internetretten, side 688-700

om at man indtaster kontooplysninger til udbetaling af overskydende skat. Når offeret indtaster oplysningerne, da kan gerningsmanden anvende disse oplysninger til en uberettiget formueforskydelse ved at give sig selv eller en anden en vinding, mens offeret lider et tilsvarende tab.
at berige sig selv ved for eksempel at lave indkøb på internettet.
Beskyttelsen mod anvendelse er delvis omfattet af de ovenfornævnte bestemmelser, og af bedrageri, jf. § 279.[18]

4.3.4 Videregivelse af informationer

Som der kommer til udtryk i afsnittet om data og information, giver information viden. Denne viden danner grundlag for en eventuel senere økonomisk fordel, hvis den bliver anvendt erhvervsmæssigt. Der er derfor stor efterregning efter visse former for information. Information kan som netop skrevet, opnås gennem en uberettiget adgang, men i stedet for selv at anvende informationen, kan det for nogen være mere fordelagtigt at videregive eller sælge denne information til en anden. De informationer som særligt nyder strafferetlig beskyttelse, er informationer som er fremkommet uberettiget, og kan for eksempel være erhvervshemmeligheder eller ikke-offentlige tilgængelig information, som kommer i hænderne på en journalist.

Det strafferetlige værn mod videregivelse af informationen er § 264c, med mindre informationen har en tilknytning til et fysisk medie, da vil § 290 i så fald kunne finder anvendelse. § 264c omfatter dog kun information som er fremkommet efter en handling som er omfattet af gerningsindholdet i §§ 263-264a.[19]

4.3.5 Særligt om erhvervshemmeligheder

Erhvervshemmeligheder kan være kendskab til kunder, leverandører og markedsanalyser og andre kommercielle forhold. Det kan endvidere handle om tekniske foranstaltninger vedrørende produktion, en ikke patenteret opfindelse eller know-how. Det kan også være produktionsmetoder, der som sådan ikke er ukendt for en fagmand, men som for virksomheden alligevel er værd at holde hemmelig. Sammenfattende er en erhvervshemmelighed, enhver forhold, som har en reel interesse i at blive holdt hemmeligt, men det formodes at oplysningen kræves at have en formueværdi, idet systemet om erhvervshemmeligheder sker på baggrund af systemet om markedsøkonomi.
Udenfor beskyttelsen som erhvervshemmelighed, er viden som er almindeligt kendt i branchen, og almindelige kundskaber som opnås i forbindelse med at drive virksomheden. Derudover udvides beskyttelsen også til at omfatte tekniske tegninger, beskrivelser, opskrifter, modeller og lignende, som ikke i sig selv er forretningshemmeligheder. Erhvervshemmeligheder omfatter ikke mundtlige instruktioner, og heller ikke al skriftlig materiale, såsom regnskab, på trods af at dette måtte indeholde informationer. En sidste begrænsning forelægger i forhold til de immaterielle

[18] Internetretten, side 719-722
[19] Kommenteret straffelov - specielle del, side 453-455

rettigheder, hvor den person der for eksempel en ophavsretlig beskyttelse i form af et edb-program, ikke af en virksomhed kan hindres i at lade andre benytte programmet også. [20]

Disse nyder en særlig beskyttelse ud over den der kommer til udtryk i straffeloven, igennem markedsføringslovens § 19, og begrebet skal også forstås i overensstemmelse med denne lov.
Markedsføringslovens § 19 forbyder ansatte i at skaffe sig adgang til erhvervshemmeligheder, jf. stk. 1, samt ubeføjet at anvende eller tilegne sig erhvervshemmeligheder på baggrund af en berettiget adgang, jf. stk. 2.
Erhvervshemmeligheder nyder dermed en beskyttelse i civilretten, mod den der har en berettiget adgang. Straffelovens § 299a supplerer mfl. § 19 med en højere strafferamme, når overtrædelsen er sket under særligt skærpende omstændigheder, herunder betydelig skade eller nærliggende fare herfor.
Derudover suppleres den uberettigede adgang med straffelovens § 263, stk. 3, som tager særligt sigte på at beskytte erhvervshemmeligheder, mod den, der uberettiget skaffer sig adgang hertil.[21]

4.3.6 Andre bestemmelser

Ud over den ovenstående inddeling i fire kategorier, er også andre bestemmelser i straffeloven tilføjet eller tilpasset til den teknologiske udvikling.
Det er blandt andet § 279a om databedrageri, § 169a om elektroniske penge, ordlydsændring til "skriftlig eller elektronisk" i § 171, stk. 2 og så strafskærpelse til immaterielle rettigheder i § 299b.

4.4 Gældende rets beskyttelse af data

I dette afsnit vil det med udgangspunkt i IT-kriminalitet, blive analyseret hvordan data beskyttes mod hærværk ud fra gældende ret.

4.4.1 § 291 om Hærværk

I hærværksbestemmelsen beskyttes en andens ting. Det er begrænset hvad der står i forarbejderne om ting, men i straffelovsbetænkningen fra 1923 udtrykkes det, at ting omfatter løsøre og fast ejendom. I den kommenterede straffelov står der, at ting må forstås som enhver art af fysiske genstande.
Ting kan fortolkes ud fra ordlyden, således ting er en fysisk genstand, eller ting kan fortolkes meget bredt, således ting er et dynamisk begreb uden fysiske grænser.
Det er op til domstolen at fortolke tingsbegrebet, og det har ført til en bred anvendelse af bestemmelsen. I U.1985.315H blev dyr omfattet af ting. Sagen handler om nedskydning af en andens hund, hvilket blev anset for hærværk. I U.1965.535V blev grøftegravning på en andens grund anset for hærværk. Bestemmelsen er dermed tidligere blevet fortolket meget bredt ud fra formålet med bestemmelsen, nemlig at beskytte en andens formuegode.

[20] Skatteret Erhvervsret, Erhvervsspionage, side 96-98
[21] Kommenteret straffelov - specielle del, side 443-444 og 616

I forhold til edb-programmer og data, som er særligt relevant for dette speciale, er der en del usikkerhed om hvor langt bestemmelsen kan strækkes, idet data ikke selvstændigt er en fysisk ting, men dog i høj grad har en særlig tilknytning til fysiske ting. Denne problemstilling har særligt været diskuteret i forbindelse med straffelovens revidering på baggrund af den nye teknologi.[22]

4.4.2 En afledt beskyttelse af ting

I 1984 anmodede justitsministeriet straffelovrådet om at tage stilling til om de gældende straffebestemmelser var tilstrækkelig til også at omfatte datakriminalitet. Strafferådet lavede derfor en udtalelses herom.
Udvalget diskuterede i forhold til hærværksbestemmelsen, hvad der var omfattet af ting i formueforbrydelserne. I forhold til tyveri, hvor der omtales en fremmed rørlig ting, som skal borttages, var der ikke tvivl om, at tingen skulle have være fysisk genstand, der kan flyttes. Dernæst diskuterede man tingsbegrebet i hærværksbestemmelsen, som ikke ud fra ordlyden skulle være rørlig. Rådet kom dog alligevel frem til den konklusion, at tingen skal være en genstand man kan tage og føle på. Rådet udtaler at dataanlæg og dele heraf, såsom lagringsmidler, dataprogrammer i fysisk form og lignende klart var omfattet af tingsbegrebet.
Dernæst diskuterede straffelovrådet om beskadigelse eller ødelæggelse af lagrede programmer var ting. Handlingen betyder, at der sker indgreb i systemets mindste enhed, hvor data lagres som magnetiske impulser, hvoraf de kan kaldes frem ved aktivering. Rådet mente at såfremt domstolen skulle træffe afgørelse i en principiel sag, ville domstolen lade lagrede programmer være omfattet af ting. Argumentet herfor var dog, at det i sidste ende stadig vil være den fysiske ting i form af lagringsenheden der ændres eller slettes og dermed beskadiges som en fysisk ting. Lagringsmediet ville herefter ikke længere indeholde den forventede data, og ville derfor være beskadiget. Dette på trods af, at lagringsmediet derefter har plads til nye data og på trods af en eventuel sikkerhedskopi. Straffelovrådet mener der er tale om hærværk efter § 291 og ikke § 293, stk. 2, uanset om indholdet er helt eller delvis slettet, og uanset om dataen er gjort midlertidig utilgængelig.
I forhold til fuldbyrdelsestidspunktet, sker det beskadigelsen allerede ved ændringen af mediet, og ikke ved den reelle ødelæggelse. Det kan illustreres med en logisk bombe, som er en tilføjelse af data, der på et senere tidspunkt sletter hele eller dele af indholdet.
Straffelovrådet overvejede også data under transmission, og udelukkede ikke at i sådan et tilfælde, ville domstolen udvide fortolkningen og anvende § 291, men ellers kunne § 263 om lukkede meddelelser anvendes.[23]

I 1987 kom den første sag for domstolen om datahærværk. I sagen var to personer tiltalt for hærværk, fordi de havde fortaget ændringer i programmer i en fagforenings dataanlæg. Ændringerne bevirkede at dataanlægget først ikke kunne udskrive dagpengechecks og efter et stykke tid, kunne dataanlægget ikke benyttes. Derudover skete der ødelæggelse på baggrund af kørsel af et program som var udlånt af den ene tiltalte. Der blev dømt for hærværk, idet der var sket ødelæggelse

[22] Kommateret straffelov - specielle del, side 592
[23] Betænkning nr. 1032 fra 1985, side 5, 30, 36-39

af en ting, nemlig fagforeningens edb-anlæg. Domstolen tolkede tingsbegrebet, som det var udtrykt i betænkningen fra 1985, nemlig at ødelæggelse af programmer, var ødelæggelse af det bærende medie. Edb-anlæggene kunne ikke anvendes efter deres formål, uden særlige foranstaltninger og derfor var der tale om hærværk af betydeligt omfang efter § 291, stk. 2. [24]
Dommen bekræftede konklusionen om at data *kun* har en afledt beskyttelse, og har dermed fortolket ting indskrænkende. Domstolens fortolkning af ordlyden skete på baggrund af betænkningens overvejelser, hvilket ifølge det tidligere afsnit om fortolkning og analogi er forventeligt.

I 1997 blev justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet nedsat. Formålet med udvalget var igen at vurdere udviklingen at de ændrede økonomiske kriminalitetsmønstre og den moderne teknologi.
Udvalget diskuterede i den forbindelse også hærværksbestemmelsens anvendelse. Udvalget så tilbage på straffelovrådets udtalelse og vurderede derfor også den afledte beskyttelse, som data nyder.
Udvalget kom frem til, at det i hvert fald overvejende måtte antages at data nød beskyttelse mod hærværk efter § 291, men denne beskyttelse kunne dog ikke siges at være utvivlsom i alle tilfælde. Udvalget ender med at konkludere at § 291 er tilstrækkelig dækkende, men at der er områder hvor data ikke er klart dækket. Der fandtes dog ikke et behov for en ny datahærværksbestemmelse og ej heller behov for at ændre i den eksisterende hærværksbestemmelse.[25]

Det er bemærkelsesværdigt at udvalget i 2002 ikke finder hærværksbestemmelsen tilstrækkeligt klart dækkende, men alligevel ikke tilføjer eller ændrer i straffeloven.
Når udvalget fra 1985 og 2002 er tilfreds med den afledte beskyttelse, og der indtil nu stadig ikke har være nogen principiel dom om datahærværk, skyldes det enten at denne fortolkning om en afledt beskyttelse er tilstrækkelig, at der endnu ikke har været et reelt angreb på data udenfor det området som er klart dækket, eller at anklagemyndigheden ikke tilstrækkeligt klart kan finde hjemmel i en bestemmelse til at løfte bevisbyrden.

4.5 Udfordringer for den afledte beskyttelse

Når data nyder beskyttelse mod hærværk, forudsætter gældende ret at data er lagret på et fysisk medie. Dermed nyder dataen en afledt beskyttelse af denne ”ting” som er beskyttelsesobjektet for § 291 og § 293. Spørgsmålet er så om denne afledte beskyttelse er tilstrækkelig.
I forhold til elektronisk lagret data er der nogle tekniske udfordringer, samt et krav om en særskilt beskyttelse af elektronisk data i cybercrime-konventionen.
Ikke-elektronisk lagret data nyder ligeledes en afledt beskyttelse, som det kom til udtryk i et forrige afsnit, men denne er dog ikke udfordret yderligere af den teknologiske udvikling.

[24] U.1987.216Ø
[25] Betænkning nr. 1417 fra 2002, pkt. 1.1, 6.1, 6.6

4.5.1 Ny teknik

Som dette afsnit vil vise, så er der på grund af internettets mange muligheder, en usikkerhed om hvorvidt data nyder den tilsigtede beskyttelse, når dataen ikke længere er knyttet til et fysisk medie.

4.5.1.1 Cloud computing

Cloud computing er en ny og populær metode at lagre sine data på. Cloud computing betyder at virksomheder og privat, kan spare penge og plads på computerressourcer i form af blandt andet lagringsplads og vedligeholdelse. Disse ressourcer bliver i stedet for stillet til rådighed hos en udbyder af lagringsplads. Nogle kendte eksempler på en sådan udbyder er dropbox eller onedrive, som begge er udbydere der stiller begrænses gratis lagringsplads til rådighed, med mulighed for at købe mere plads. Når data lagres ved en udbyder, har brugeren stadig en let adgang til sine data, idet ethvert datasystem med internetadgang og som er kompatibel med udbyderens system, kan oprette forbindelse til den eksterne lagringsplads ved brug af brugernavn og adgangskode. Denne mulighed for lagring af data på en online servere, betyder også at brugeren har adgang til sine data, uanset hvor i verden han er. Der er derfor flere grunde til, at der sker en hurtig udvikling indenfor cloud computing.

Lagring af informationer kan som tidligere skrevet ske direkte på papir eller digitalt på en harddisk. Begge muligheder rummes så vidt muligt af de samme bestemmelser med enkelte tilpasninger. På grund af cloud computing, udfordres lovgivningen dog endnu engang af den digitale udvikling, fordi cloud computing ikke har tilknytning til et bestemt fysisk medie, som er brugeren bekendt. Dataen kan af udbyderen blive flyttet mellem flere servere, uden brugeren bemærker det. Brugerens oplevelse er at dataen opbevares i en sky, deraf ”cloud computing”.

Når cloud computing anvendes, er det ikke den samme person, der har ejendomsretten til den lagrede data som den der har ejendomsretten til det bærende medie. Dette kan eventuelt give problemer i forhold til påtalekompetencen i forbindelse med ødelæggelse af dataen.

Påtalekompetence

Som det fremgår af straffelovens § 305, sker der kun påtale hvis den forurettede begærer det eller almene hensyn kræver påtale. Den forurettede er den der ejer tingen, fordi beskyttelsesobjektet i hærværksbestemmelsen er ting.[26] En afledt beskyttelse betyder dermed, at når data udsættes for hærværk, er det som udgangspunkt den, der har ejendomsretten til det bærende medie, som er den forurettede.

Det virker i sådan et tilfælde utilstrækkeligt at give data en afledt beskyttelse, blandt andet fordi det ofte er dataen, der er angrebsobjektet og ikke det bærende medie.

Man kunne forestille sig, at den der lejer lagerplads, har en sådan interesse i det fysiske medie, at denne også bliver forurettede. Problemet har ikke tidligere være så relevant, idet det oftest var den samme, som havde ejendomsretten til den lagrede data, som havde ejendomsretten til det bærende medie.

[26] Private straffesager, side 191

Opstår der en situation, hvor det er den, der har ejendomsretten til det bærende medie, der som forurettede har påtalekompetencen, opstår der et problem for den, der har ejendomsretten til data, såfremt den med påtalekompetencen ikke har til hensigt at anmelde for hærværk. Det kan der være flere grunde til, blandt andet ønsket om ikke at få sin virksomheds hærværksangreb offentliggjort.[27]

Norges overvejelser

Inger Marie Sunde skriver i sin afhandling om det norske funktionelle genstandsbegreb, at der ikke er tilstrækkelig beskyttelse, når den der har ejendomsretten til dataen, ikke er den samme som den der har ejendomsretten til det bærende medie. Det begrunder hun blandt andet med at der i den norske bestænkning fra 1985, står at ændring og sletning fører til at lagringsmediet for ejeren ikke er det samme som før ændringen eller sletningen. Når en anden lagrer sine data på ejerens medie, rammes ejeren ikke af hærværk, da mediet for ejeren, er i samme stand før angrebet, som efter. Ejeren af netværksserveren rammes altså ikke, når ejeren af data rammes. Der kan derimod være tale om en forbrydelse mod lejeren, der rammes allerede af § 263, stk. 2 om uberettiget adgang, idet denne bestemmelse beskytter informationerne.
Inger Marie Sunde mener heller ikke at ejeren af data udsættes for datahærværk, såfremt ejeren af det bærende medie sletter dataen, idet det som nævn ikke sker en ændring for ejeren af det bærende medie.[28]

I den danske betænkningen fra 1985, har straffelovrådet overvejet den situation, hvor ejeren af en server uberettiget skaffer sig adgang til lejerens data. I sådan en situation sker der en strafbar krænkelse af lejerens interesse og der kan straffes for uberettiget adgang efter § 263, stk. 2.[29] Disse overvejelser er de eneste om en andens data på egne servere, og problemstillingen om hærværk af andres data på egne lagrer er altså ikke overvejet.

Forurettede

Hvem der er forurettede, er ikke defineret i straffeloven. Spørgsmålet er så, om den forurettede også kan være den der lagrer data, idet denne har en interesse i at beskytte disse.
Denne problemstilling er er et processuelt spørgsmål, og derfor må svaret i første omgang søges i retsplejeloven. Retsplejelovens § 725, siger at retten til privat påtale, samt retten til at fremsætte begæring om offentlig påtale, tilkommer den forurettede, men det fremgår ej heller af denne lov, hvem den forurettede er. I betænkning nr. 1485 fra 2006 om forurettedes processuelle retsstilling i straffesager, står der heller ikke klart hvem forurettede er. Betænkningen henviser til litteraturen, hvoraf det fremgår at det må fortolkes forholdsvis snævert, hvem der er den forurettede. I de fleste tilfælde er det ikke problematisk at finde frem til, hvem der er den forurettede, idet der ty-

[27] TfK.2013.240, pkt. 1, 2, 3.1.1.1
[28] Automatisert inndragning, side 148-149
[29] Betænkning nr. 1032 fra 1985, side 26

pisk fremgår af straffebestemmelserne, hvem beskyttelsesobjektet er. Der henvises især til forbrydelser mod kønssædeligheden, samt forbrydelser mod liv og legeme.
Det kommer derudover til udtryk i betænkningen, at afgrænsningen af hvem der er forurettede, kan være forskellig, alt efter hvordan udtrykket anvendes. Drejer den konkrette sag sig om et borgerligt krav, kan begrebet udvides til at være forsikringsselskaber eller tredjemand, som skal have dækket et krav for den oprindelige forurettede.[30]
Beskyttelsesobjektet i straffelovens § 291 er som nævnt *en andens ting*. Forurettede må derfor som udgangspunkt være ejeren af tingen. Hvis tingen, der udsættes for hærværk er en bil, da må det være bilens ejer der er påtaleberettiget efter § 305 og ikke alle bilens brugere.
Fra retspraksis kan dog nævnes TfK.2001.177/2, hvor tiltalte smadrede forruden i en taxa. Chaufføren anmeldte forholdet og begærede tiltalte straffet, samt krævede chaufføren erstatning for ruden. Tiltalte påstod frifindelse, idet chaufføren ikke var påtaleberettiget.
Byretten fandt at der var fornøden grundlag for påtalen, da det af politirapporten fremgik at chaufføren på vognmandens vegne ønskede tiltalte straffet samt erstattet ruden. Landsretten kom frem til samme resultat, idet der ikke som betingelse kan stilles af ejeren af taxaen personligt tiltræder påtalebegæringen eller at politiet sikrer at chaufføren havde haft den fornødne fuldmagt.[31]
I dommen U.2003.1907Ø havde tiltalte sparket en dør i stykker i en butik samt udøvet vold mod en ansat i butikken. I byretten blev tiltalte frifundet for hærværk af døren, idet der ikke var påtalekompetence. I landsretten kom man frem til at butikschefen i politirapporten havde begæret tiltalte straffet og erstatningsansvarlig. Butikschefen havde ligeledes fremsendt en opgørelse på erstatningskravet.[32]
Som det fremgår af dommene, er det ikke tilstrækkeligt klart, hvem der som udgangspunkt er den forurettede. De ovenstående domme, som dog ikke omhandler IT-kriminalitet, illustrerer at ikke enhver interesse er tilstrækkelig for at rejse tiltale, men at det ikke er udelukket at andre end ejeren kan rejse påtale.

Når der i gældende ret argumenteres for, at ændring af data er en omstrukturering af magnetiske impulser på en fysisk ting, som derfor er hærværk af det bærende medie, peger det netop på, at den forurettede er ejeren af det bærende medie. Det skyldes at data i sig selv, endnu ikke direkte har haft en beskyttelse mod hærværk, og har dermed ikke været beskyttelsesobjektet i § 291. Omvendt har ejeren af dataen en interesse, som i mange tilfælde er støre end den interesse som ejeren af serveren har, hvilket taler for at denne har en påtalekompetence.
Som det fremgår heraf, er der et behov for en tydeliggørelse af den selvstændige beskyttelse af data. Det kan enten være i form af en klar fortolkning af ting, der således også omfatter data selvstændigt, eller det kan være en lovændring, som tilføjer data som selvstændigt beskyttelsesobjekt

[30] Betænkning nr. 1485 fra 2006, side 16-17
[31] TfK.2001.177/2
[32] U.2003.1907Ø

i hærværksbestemmelsen. På den måde vil der ikke være tvivl om hvorvidt data er tilstrækkeligt beskyttet og dermed, om der er påtalekompetence når dataen lagres på en andens server.

4.5.1.2 Data under transmission

Data er i stigende grad under transmission, både som e-mails og som overførsler fra online servere i forbindelse med ekstern lagring eller køb af information og programmer.
Når gældende ret giver data en afledt beskyttelse af det bærende medie, er spørgsmålet om data nyder beskyttelse, når data er under transmission.
I det fleste tilfælde, hvor dataen ændres undervejs, vil dataen være beskyttet allerede fordi, en adgang til denne data vil være uberettiget. Data er derfor beskyttet af den eksisterende hackerbestemmelse i straffelovens § 263, stk. 2.[33]
Såfremt man forestiller sig en situation, hvor gerningsmanden har en berettiget adgang til dataen, opstår der dog en situation lignende den, som er gældende for cloud computing, nemlig at data muligvis ikke er tilstrækkeligt beskyttet. Det er svært at forestille sig et konkret eksempel, men såfremt mail-klienten sletter brugernes mails, er situationen lignende den, som Inger Marie Sunde ovenfor gjorde gældende om data på en andens server.

4.5.2 Cybercrime-konventionens særskilte beskyttelse

Cybercrime-konventionen har særskilte artikler om beskyttelse af henholdsvis data i artikel 4 og edb-systemer i artikel 5. Det virker derfor utilstrækkeligt at dansk ret ikke også giver en klar selvstændig beskyttelse til data, men derimod en afledt beskyttelse af systemet og det bærende medie.
Som der er redegjort for i et tidligere afsnit om datakriminalitet, er systemet beskyttet allerede af §§ 193, 291 og 293, mens data kun har en afledt beskyttelse. Den afledte beskyttelse begrundes i, at systemet ikke længere fungere efter hensigten, og spørgsmålet er så, om det i sidste ende ikke stadig er systemet der beskyttes.
I næste afsnit vil muligheden for en udvidet fortolkning af ting blive analyseret, og såfremt data selvstændigt kan fortolkes som ting, opfylder hærværksbestemmelsen uden tvivl kravet om at give data den beskyttelse som konventionen kræver. Hvis det viser sig at fortolkningen kommer i konflikt med det strafferetlige legalitetsprincip, må en ny bestemmelse eller en regulering af de eksisterende bestemmelser overvejes, således national ret er i overensstemmelse med Cybercrime-konventionen. [34]

4.6 Fortolkning af ting i forhold til data

Det er ikke til at sige om der sker en udvidet eller indskrænkende fortolkning af ting, såfremt domstolen bliver spurgt om data er direkte omfattet ting.
I dette afsnit bliver tingsbegrebet i § 291 fortolket ud fra de principper, der blev gjort gældende i det tidligere afsnit om fortolkning af straffelovens legalitetsprincip.

[33] Betænkning nr. 1032 fra 1985, side 38-39
[34] TfK.2013.240, pkt. 3.1.2

Formålet med dette afsnit, er at hjælpe til at vurdere, om data er tilstrækkeligt beskyttet efter de nugældende bestemmelser, eller om en lovændring er at foretrække.

Fortolkningen i dette afsnit sker på baggrund af de tidligere nævnte principper, om ordlyds- formåls-, straf- og limitationsfortolkning, for at se om der er mulighed for en udvidet fortolkning.
I betænkning nr. 1485 fra 2002 står der, at det ikke er udelukket, at data fortolkes som ting i en eventuel principiel sag, men i dette afsnit undersøges alligevel muligheden for denne udvidet fortolkning, idet en udvidet fortolkning skal respektere legalitetsprincippet. Derudover undersøges muligheden for at ændre den tidligere fortolkning om en afledt beskyttelse til en direkte beskyttelse.

4.6.1 Ordlydsfortolkning

Ordlyden skal fortolkes ud fra hvad der er er almen anerkendt forståelse af ordet. Det er ikke klart hvad der forstås med ting, og forarbejderne siger som nævnt kun, at ting er løsøre og fast ejendom.
Ting skal i første omgang fortolkes ud fra, hvad straffelovens øvrige bestemmelser forstår ved ting. Når begrebet går igen flere steder i loven, må man gå ud fra at det også skal forstås ens. Hvis dette ikke er tilstrækkeligt, må den øvrige lovgivning inddrages. [35]

Ting er beskyttelsesobjektet i tyveribestemmelserne §§ 276-278, i § 291 om hærværk og § 293 om brugstyveri. Derudover anvendes begrebet "udbytte" i § 290 om hæleri, som omfatter penge og genstande. Formålet med at analysere alle disse bestemmelser, er at finde frem til hvordan strafferetten overordnet set behandler ting, for dernæst at kunne vurdere om data og information er tilstrækkeligt klart omfattet af tingsbegrebet i § 291 om hærværk.

4.6.1.1 § 276 – 278 om tyveri, hittegods og underslæb af "fremmed rørlig ting"

Bestemmelserne om tyveri, ulovlig omgang med hittegods og underslæb, beskytter en "fremmed rørlig ting" Der er derfor en lighed mellem disse bestemmelser og hærværksbestemmelsen, som beskytter en "andens ting". Som det kommer til udtryk direkte i ordlyden, skal tingen være rørlig, dermed udelukkes varemærker, navne og lignende. Tilegnelse af erhvervshemmeligheder er ligeledes udelukket fra tyveri, når det sker som afskrift eller kopiering. I § 276, stk. 2 sidestilles energimængder med ting, som er fremstillet, opbevaret eller taget i brug i økonomisk øjemed.
Bestemmelserne er alle taget med under et, fordi det eneste der adskiller bestemmelser fra hinanden, er varetægtsforholdet. I § 276 skal tingen være i en andens varetægt, i § 277 er tingen ikke i nogens varetægt og i § 278 er tingen i egen varetægt. Dette illustrerer dermed også hvordan respekten for det strafferetlige legalitetsprincip er kommet særligt til udtryk i bestemmelser om at tilegne sig en andens ting.
Bestemmelsen er her taget med, for at illustrere at andre bestemmelser om ting, som utvivlsomt skal være fysisk, har denne betingelse med i ordlyden, og ikke ladet spørgsmålet være åben for fortolkning som i § 291.[36]

[35] Justitsministeriets vejledning nr. 224 af 15. Oktober 1969, pkt. 1

4.6.1.2 § 290 om hæleri af "udbytte"

Hæleri straffer efter § 290, den som uberettiget modtager eller skaffer sig del i udbytte, eller uberettiget skjuler, opbevarer, transporterer, hjælper til at afhænde eller på anden måde sikrer en anden et udbyttet. Der er ingen krav om hvilken forbrydelse, som lægger forud for hæleriet, og kan derfor som udgangspunkt anvendes mod alle før-forbrydelser.
I kommentaren til § 290 står der at et udbytte kan være en genstand. Bestemmelsen er derfor her taget med, idet genstand og ting må forstås ens ud fra en almindelig fortolkning af ordet.[37] I kommentaren står der dog også, at informationer ikke er omfattet af genstandsbegrebet, såfremt de ikke er knyttet til et fysisk medie, men i stedet for kan man i nogle situationer anvende § 264c.

§ 264c kaldes også for informationshæleri. Bestemmelsen straffer den, der uden at have medvirket selv, skaffer sig eller uberettiget udnytter oplysninger som er fremkommet af en forbrydelse efter §§ 263, 264 eller 264a.
Bestemmelsen er en form for efterfølgende medvirken, som sikrer at eksempelvis en person ikke anvender oplysninger, som en anden gerningsmand har skaffet sig uberettiget adgang til. [38]

Ved retten i Hjørring den 15. januar 2013 blev den taltalte frifundet for hæleri af pinkodeoplysninger og personlige kundeoplysninger. Dommen handler om en tiltalt, som under afsoning af frihedsstraf for en tidligere forbrydelse, var kommet i besiddelse af 9873 sæt personlige oplysninger, som stammede fra en strafbar handling, samt oplysninger, som identificerede et betalingsmiddel. Byretten henviste til forarbejderne til hæleribestemmelsen, som udtrykker at udbytte ikke omfatter informationer. Retten frifandt derfor for disse to forhold. Rettens begrundelse var at det måtte antages, at informationerne var kommet fra internettet, og derfor ikke var knyttet til et fysisk medie. Dermed kunne der ikke straffes for hæleri efter § 290. [39]
Når anklagemyndigheden tiltalte for hæleri efter § 290 i stedet for § 264c, var det fordi det ikke kunne bevises at informationerne var fremkommet ved en af de nævnte før-forbrydelser.

Dommen viser hvordan domstolen i 2013 stadig benytter den indskrænkende fortolkning om at data er informationer, som har en afledt beskyttelse, og altså ikke er omfattet af tings- eller genstandsbegrebet. Havde domstolen i stedet for fortolket hæleribestemmelsen ud fra bestemmelsens formålet, er det ikke usandsynligt at domstolen var kommet frem til et andet resultat, idet formålet er at straffe den der uberettiget modtager eller skaffer sig del i udbytte.
Dommen viser også hvordan elektronisk data i nogle situationer ikke nyder en tilstrækkelig beskyttelse, fordi data der befinder sig på internettet, ikke er tilknytning til et fysisk medie.

4.6.1.3 § 293 om brugstyveri af "ting"

Brugstyveri straffer den, der uberettiget bruger en ting, der tilhører en anden. Efter stk. 2 straffes også den der uberettiget helt eller delvis hindrer en anden i at råde over ting.

---

[36] Kommenteret straffelov – specielle del, side 513-522
[37] http://ordnet.dk/ddo/ordbog?query=ting&search=Søg
[38] Kommenteret straffelov – specielle del, side 585-587
[39] Dom afsagt ved Retten i Hjørring, den 15. januar 2013

Bestemmelsen fik en ordlydsændring i 2004, da den tidligere formulering straffede den, der lægger ting i vejen. Formålet med ændringen var at fremhæve at ikke kun fysiske hindringer, men også elektroniske hindringer er omfattet.
I forhold til IT-kriminalitet kan stk. 1 anvendes, når en person bruger en andens system til at foretage egne opgaver, eller hvis gerningsmanden skaffer sig adgang til et andet system for at kopiere informationer og programmer. Bestemmelsen kan også bruges hvis gerningsmanden anvender den andens computer til at udfører Dos-angreb og andre angreb mod et tredje system.
At brugen skal være uberettiget kan i arbejdsforhold give problemstillinger, som konkret må afgøres ud fra om der er tale om brugstyveri. I nogle tilfælde er det aftalt at arbejdsgiverens computer må anvendes privat, mens der i andre tilfælde er der ingen aftale herom. [40]
Bestemmelsens stk. 2 anvendes i nogle tilfælde i stedet for hærværksbestemmelsen, blandt andet i den situation hvor gerningsmanden ved at anvende en virus, hindrer den retmæssige bruger i at anvende sine elektronisk lagrede data, såfremt dette medfører at systemet for gerningsmanden ikke længere fungere efter hensigten.[41]

Beskyttelsesobjektet er ligesom i hærværksbestemmelsen en ting, og i modsætningen til §§ 276-278 kommer der ikke direkte til udtryk i ordlyden, at tingen skal være rørlig. Brug af edb-system eller dele heraf er brug af en andens ting. I dommen U.2003.1950Ø blev politiets server anvendt til lagring af pornografiske billeder, og dette var brugstyveri efter § 293, stk. 1, fordi serveren, som en fysisk ting blev brugt. Det kommer til udtryk i kommentaren til bestemmelsen, at uberettiget brug af elektronisk lagret information ikke er brugstyveri, medmindre det er en fysisk ting, som for eksempel en diskette, som bruges uberettiget. Ting bliver dermed begrænset til kun at omfatte fysiske genstande efter stk. 1.
Bestemmelsens stk. 2 blev ændret i forbindelse med betænkningen fra 2002, fra "tilbageholde en ting" til "uberettiget hindrer". Formålet med ændringen var at ramme den elektroniske hindring, som bevirker at systemet ikke fungerer. Som det kom til udtryk i det tidligere afsnit om informationskriminalitet, er det typisk DoS-angreb, som bevirker at edb-systemet ikke fungere, og dermed er ting i stk. 2 også afgrænset til en fysisk genstand.[42]

4.6.1.4 Købelovens løsørebegreb

Straffelovens andre bestemmelser, som indeholder ordet ting, omfatter altså som udgangspunkt ikke data, og taler derfor imod at data kan være omfattet af ting i § 291.
Ud over straffelovens bestemmelser, kan der ses på andre love, som også indeholder ordene ting, data eller løsøre. Købeloven er særligt relevant, fordi loven gælder for alle køb, bortset fra køb af fast ejendom, jf. § 1. Køb er ikke defineret i loven, men normal opfattelse er, at køb dækker over enhver aftale om overdragelse af et formuegode i form af løsøre, mod et vederlag i form af penge. Købeloven ender altså ligesom straffeloven med at skulle vurdere data i forhold til løsøre.

[40] Kommenteret straffelov - specielle del, side 597
[41] Internetretten, side 699-700
[42] Kommenteret straffelov – specielle del, side 596 - 601

Løsøre er i følge den store danske "flytbare formuegenstande". Det betyder at "ting" er en rørlig genstand med en økonomisk værdi. Købeloven er dog ikke begrænset til kun at omhandle fysisk rørlige ting, da det kommer til udtryk i lovens §19 og § 20, at også aktier og skriftlige rentebærende fordringer er omfattet.
Den opfattelse, at både fysiske og digitale informationer er omfattet af købeloven, illustreres blandt andet ved køb af en bog. Den fysiske bog er uden tvivl omfattet, da denne opfylder betingelsen for at være et løsøre. Den samme bog kan oftest også købes digitalt, og dette køb vil også være omfattet af købeloven. Spørgsmålet er så om alle former for information er omfattet af købeloven. Hvis den omtalte bog indeholder vittigheder, som både er omfattet af købeloven i bogform og som digital download, opstår spørgsmålet om bogen også er omfattet, hvis vittighederne bliver overdraget mundtligt. Der er ingen tvivl om, at en mundtlig overdragelse af informationer, ligger langt fra købelovens hovedområde, men omvendt er der ingen reelle grunde til, at dette køb ikke også skulle være omfattet.
Data som elektronisk lagret information, er altså derfor omfattet af købeloven, som efter den almindelige opfattelse omhandler køb af løsøre. [43]
Selvstændigt siger dette ikke, om data er omfattet af tingsbegrebet i hærværksbestemmelsen, men idet reglerne om fortolkning af straffelovens ordlyd, som udgangspunkt ikke er anderledes end andre fortolkningsregler, taler det for at data kan være omfattet af ting.

4.6.2 Formålsfortolkning

Ud over en fortolkning af ordlyden, kan fortolkningen også ske ud fra beskyttelsesinteressen.
Ud fra hærværksbestemmelsens placering i straffelovens kapitel 28, er beskyttelsesinteressen et formuegode. Når hærværk beskytter ting, må ting som udgangspunkt kunne fortolkes som ethvert formuegode. Data kan have en betydelig værdi, for blandt andet virksomheder, i form af erhvervshemmeligheder, der kan være lagret digitalt eller fysisk.
På trods af bestemmelsens placering i straffelovens kapitel 28 om formueforbrydelser, er der dog ud fra litteraturen, ikke et krav om at tingen skal have en værdi.[44]

Inger Marie Sunde mener, at det norske genstandsbegrebet, som er sammenligneligt med ting, er dynamisk og dermed skal forstås udvidende. Bestemmelserne skal forstås udvidende ud fra formål og ikke indskrænkende ud fra begrebet, som ikke kunne forudse den teknologiske udvikling. Data skal derfor som udgangspunkt altid være omfattet af genstandsbegrebet, men i de bestemmelser hvor data ud fra bestemmelsens formål ikke kan være omfattet, såsom ved tyveri, da må disse bestemmelsen fortolkes indskrænkende. Hun mener også at det vil være utilstrækkeligt, såfremt data ikke er ting, blandt andet i situationer hvor data ikke har en fast tilknytning til et fysisk me-

[43] IT-retten, side 444-446
[44] Kommenteret straffelov – specielle del, side 592

die.[45] I forhold til cybercrime-konventionens selvstændige artikel som beskytter data, vil det ligeledes virke utilstrækkeligt, såfremt data ikke er ting.[46]

4.6.3 Straffortolkning

Strafferammen for hærværk strækker sig fra bøde til halvandet års fængsel med skærpelse til 6 års fængsel i særlige tilfælde. Det betyder, at der er en meget bred strafferamme, men i forbindelse med almindeligt hærværk, er strafferammen forholdsvis mild. Selv om denne fortolkningsmetode er begrænset anvendelig, støtter denne op om, at data kan være omfattet af ting.

4.6.4 Limitationsfortolkning

Hærværksbestemmelsen er kun afgrænset af få bestemmelser om blandt andet ildspåsættelse og sprængning. Derudover er der særbestemmelser om hærværk af ophavsretlige værker, men i forhold til data, er der ingen særbestemmelser. Databedrageri er særligt anvendelig, når data ødelægges, men denne bestemmelse forudsætter at der er en økonomisk vinding for gerningsmanden.

Der er samlet set stor sandsynlighed for, at data er ting ud fra en udvidet fortolkning af bestemmelsen. Så længe det ikke står klart i litteraturen, kommentaren eller i betænkningerne, er det dog op til domstolen at udvide denne fortolkning. Det forudsætter dog at domstolen ikke er bundet af den allerede indskrænkede fortolkning fra 1987, der som den eneste har taget direkte stilling hertil. Spørgsmålet er altså om denne dom har præjudikatsværdi.

4.6.5 Lighedsbetragtning

Lighedsbetragtningen betyder, at domstolen så vidt muligt dømme ens, således borgeren i retssamfundet har en forudsigelighed i hvad der er strafbart.
Da domstolen i 1987 tog stilling til om data var ting, var der også mulighed for den ovenstående udvidet fortolkning, men domstolen fandt den afledte beskyttelse tilstrækkelig.
Domstolen er dog ikke bundet af en tidligere fortolkning, fordi domstolen ikke skal dømme forkert, såfremt den tidligere fortolkning ikke længere viser sig at være korrekt.
Domstolen er som kendt i tre instanser, og en højere instans er aldrig bundet af en tidligere, eller en sidestående instans. Det betyder at byretter ikke behøver at dømme ens, når der er tvivl om fortolkning, og at landsretten ikke nødvendigvis skal dømme som byretten, eller den anden landsret.
Hvorvidt domstolen er bundet af den højere instans i en fortolkningssituationer, er et spørgsmål om præjudikatsværdi. Oftest respekterer underinstansen den højere instans fortolkning, og ofte respekteres sidestilledes instansers afgørelser også. Især en højesteretsdom har en høj præjudikatsværdi.
Dommen om datahærværk er en landsretsdom fra 1987. Det er derfor typisk at byretterne følger denne fortolkning, så længe det er muligt. Skal byretten tage stilling til, om data i en tilsvarende

[45] Lov og rett i cyberspace, side 100-112
[46] TfK.2013.240, pkt. 3.1.2

situation er omfattet af ting, er der stor mulighed for at denne vil komme frem til samme resultat. Hvis situationen er andeledes, ved at data kun har en begrænset eller ingen tilknytning til det fysiske medie, er muligheden stor for at domstolen vælger den anden fortolkning.
Hvis domstolen i 2. Instans skulle fortolke data som værende omfattet af ting, vil denne dom med stor sandsynlighed blive gældende praksis, fordi dommen i så fald er nyere. Der er dog endnu en tredje instans, som kan tage endelig stilling til spørgsmålet om hvorvidt data er ting.[47]

Overordet set er der intet til hinder for, at ting kan blive fortolket, således data nyder en selvstændig beskyttelse. Det er dog ikke gældende ret, så længe en domstol ikke har taget endelig stilling, så indtil da er der kun en formodning for, at data er tilstrækkeligt beskyttet mod hærværk.

4.7 Tidligere lovændring af § 263

I betænkningen fra 1985 blev § 263 behandlet i forhold til IT-kriminalitet. I betænkningen henvises der til lov nr. 89 af 29. marts 1972, hvor bestemmelsen på baggrund af betænkning om privatlivets fred blev ændret. Ændringen i 1972 skete for at sikre tidens tekniske midler til aflytning, lydoptagelse, iagttagelse og fotografering tilstrækkeligt klart skulle være omfattet af bestemmelsen. I 1972 var databehandling stadig meget nyt, men ikke meget udbredt, og man vurderede at det endnu var for tidligt at regulere lovgivningen i forhold til den nye teknologi.
I 1985 havde teknologien udviklet sig tilstrækkeligt til, at § 263 måtte vurderes i forhold til uberettiget indtrængen i et edb-system, og i den forbindelse blev stk. 1 nr. 1-3 fortolket.
Bestemmelsens nr. 1 beskytter en lukket meddelelse, og man vurderede at et dataanlæg kunne afsende og modtage lukkede meddelelser, idet der i forarbejderne ikke var krav om en fysisk forseglet meddelelse. I forhold til edb-meddelelser, vurderede man, at ud fra en fortolkning kunne bestemmelsen finde anvendelse, mod den, der uberettiget skaffer sig adgang til en elektronisk meddelelse. Udvalget fandt dog at hvilende meddelelser i edb-systemet som udgangspunk ikke var omfattet af nr. 1. Udvalget sammenlignede den danske bestemmelse med den lignende norske bestemmelse, som på grund af ordlyden blev vurderet af være mere dækkende. Man udtalte, at det var sandsynligt, at den danske domstol kunne komme frem til samme resultat som den norske, men i så fald ud fra en vid fortolkning af bestemmelsen.
Bestemmelsens nr. 2 straffer den, der uberettiget skaffer sig adgang til andres gemmer. Udvalget vurderede at denne bestemmelse omfattede skuffer, skabe og andre fysiske gemmer, men at det ud fra en sproglig naturlig forståelse af ordlyden, ikke kunne omfatte uberettiget adgang til oplysninger i et edb-system.
Bestemmelsens nr. 3 er ikke formuleret således, det kan være aktuelt at bruge bestemmelsen til uberettiget adgang til et edb-system, idet bestemmelsen straffer hemmelig aflytning og lignende.

§ 264 om husfredskrænkelse blev også fortolket i forhold til edb-systemer, men da denne bestemmelse beskytter bygninger, er det således adgangen til edb-systemet i bygningen, der beskyt-

[47] Det strafferetlige legalitetsprincip, side 315-317

tes. Dermed kunne denne bestemmelse heller ikke anvendes imod uberettiget adgang til oplysningerne i edb-systemet.

Ovenstående fortolkning af §§ 263 og 264 førte til forslaget om § 263, stk. 2. Den nye bestemmelse straffer den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling. [48]
Bestemmelsen udtryk "anlæg til elektronisk databehandling" blev senere ved lov nr. 352 af 19. maj 2004 ændret til "informationssystem".

Baggrunden for indsættelsen af § 263, stk. 2, bevirker at der må overvejes en dansk tilføjelse til beskyttelse af data mod angreb- Det skyldes at situationen om en uklar retsstilling eller vid fortolkning endnu engang er problemstillingen.

4.8 Sammenfatning

I dette kapitel om gældende ret, er det blevet undersøgt hvordan data nyder beskyttelse mod hærværk. Først blev data, informationer og viden beskrevet sammen med en forklaring på hvorfor data er beskyttelsesværdig, og dernæst blev datakriminalitet beskrevet generelt, for at danne et indtryk af hvor bredt området er.
I den videre analyse af gældende ret, er hærværksbestemmelsen blevet analyseret, hvor det kom til udtryk, at data nyder en afledt beskyttelse af det bærende medie.
Den afledte beskyttelse har været anvendt til ikke-elektronisk lagret data, og da man har ønsket at behandle IT-kriminalitet ligesom almindelig kriminalitet, er den afledte beskyttelse fundet tilstrækkeligt til elektronisk lagret data også.
Når data lagres digitalt, opstår der på grund af den teknologiske udvikling, nogle situationer, som bevirker at den afledte beskyttelse ikke er tilstrækkelig. Det sker når dataen lagres på en andens server, som blandt andet sker i form af cloud computing. Cloud computing betyder af den der har ejendomsretten til dataen ikke er den samme som har ejendomsretten til det bærende medie, og da påtalekompetence i den almindelige hærværksbestemmelse er ved forurettede, opstår der tvivl om hvem der er forurettede i forbindelse med et dataangreb på en andens server.
Derudover er en afledt beskyttelse ikke tilstrækkelig i forhold til cybercrime-konventionen, som har en særskilt bestemmelse til henholdsvis data og edb-system. Cybercrime-konventionen kræver derfor, at ting fortolkes udvidende til at beskytte data selvstændigt, i stedet for en afledt beskyttelse af det bærende medie.
På baggrund af den uklare retsstilling ud fra ordlyden og de udfordringer som den afledte beskyttelse giver, er tingsbegrebet i hærværksbestemmelsen, og de bestemmelser som derudover beskytter ting, blevet fortolket ud fra de principper, som blev beskrevet i det redegørende kapitel.
Ud fra en ordlydsfortolkning er tingsbegrebet i straffeloven generelt afgrænset fra at omfatte ting. Dette udelukker dog ikke en endelig fortolkning af hærværksbestemmelsen, og i forhold til købelovens anvendelsesområde som omfatter løsøre, er det ikke udelukket at data kan være omfattet

[48] Betænkning nr. 1032 fra 1985, side 21-29

af tingsbegrebet. Ud fra formåls-, straf- og limitationsfortolkning er det heller ikke udelukket at data kan være omfattet af tingsbegrebet. Fordi en fortolkning af tingsbegrebet ikke udelukker at data kan være omfattet af tingsbegrebet, er det undersøgt om domstolen kan ændre en tidligere fortolkning. Her kom det til udtryk at domstolen respekterer sidestillede og højere retter, medmindre det på baggrund af en ny fortolkning, viser sig at være mere rigtigt med en anden fortolkning. Oftest har højesteret dog en så høj præjudikatværdi, at dennes afgørelser følges. Dermed er der intet til hinder for at domstolen, både by- og landsretterne kommer frem til, at ting skal fortolkes udvidende til også at omfatte data.
Endeligt har kapitlet analyseret tilblivelsen af hackerbestemmelsen i § 263, stk. 2. Denne bestemmelse blev føjet til straffeloven på baggrund af betænkningen fra 1985. Tilføjelsen skyldtes, at på trods af en mulighed for udvidet fortolkning af den eksisterende bestemmelse, så fremgik det ikke tilstrækkeligt klart af ordlyden, om en uberettiget adgang til en edb-system kunne være omfattet.

5. SELVSTÆNDIG BESKYTTELSE (de lege ferenda)

5.1 Indledning

Som det kom til udtryk i det forrige kapitel, fremgår det ikke klart af ordlyden og ej heller af fortolkning, om data er tilstrækkeligt beskyttet mod hærværk.

I dette afsnit vil den norske lovændring i 2004 blive analyseret. Norge tilføjede data som et selvstændigt beskyttelsesobjekt i sin hærværksbestemmelse, og da Danmark ofte ser på de andre nordiske lande i sit arbejde med lovgivningen, er Norge særligt relevant for dette speciale.

På bagrund af analysen i det forrige kapitel og den norske lovændring, foreslås en dansk lovændring til selvstændig beskyttelse af data. Forslaget til den danske lovændring er sket med inspiration fra den norske, og i persondataloven. Persondataloven omhandler databehandling af personlige oplysninger, men som det kommer til udtryk i lovens § 1, gælder denne lov både for elektronisk og ikke-elektronisk behandling af personoplysninger. I forhold til datahærværk, er det i de tidligere kapitler gjort gældende, at datakriminalitet og almindelig kriminalitet skal behandles så vidt muligt ens, og ligeledes er det kommet til udtryk, at behovet for databeskyttelse ikke afgrænser sig til elektronisk lagret data.

I forlængelse med forslaget til en dansk lovændring, følger et afsnit som analyserer konsekvenserne af en lovændring. En ny bestemmelse medfører udover en klarhed i anvendelsesområdet, også nogle andre spørgsmål som man må tage stilling til.

Formålet med kapitlet er at give et alternativ til gældende ret, således en uklar retsstilling kan ændres til en tydelig opfyldelse af det strafferetlige legalitetsprincippet.

5.2 Norsk lovændring i 2004

Norge har gennem længere tid arbejdet på en ny straffelov, som delvis er trådt i kraft. I det forberedende arbejde til den nye straffelov, var der foreslået et separat kapitel mod IT-kriminalitet. IT-kriminalitet blev vurderet i forbindelse med den nye straffelov, fordi Norge også tilsluttede sig Cybercrime-konventionen. Begrundelsen for at udvalget foreslog et særskilt kapitel mod IT-kriminalitet, var at krænkelser mod data og datasystemer rejser så mange spørgsmål, at en særregulering blev vurderet som den bedste løsning. Derudover har reglerne om datakriminalitet så meget tilfældes, blandt andet fælles begreber, at det af pædagogiske hensyn og af hensyn til overblikket, ville give bedst mening at samle bestemmelserne i et selvstændigt kapitel. Ved at tilpasse de eksisterende bestemmelser, opstår der særlige situationer og problemstillinger, som først må løses før bestemmelserne kan benyttes på IT-kriminalitet. Ved for eksempel at kriminalisere datatyveri som uberettiget kopiering eller overføring af data til datasystemer som gerningsmanden kontrollerer, skal man ikke tage stilling til begreberne ”borttager” og ”ting”, som er afgørende for den almindelige tyveribestemmelse. Definitioner som anvendes indenfor datakriminalitet, er ikke nødvendigvis lige så godt dækkende for almindelig kriminalitet. Endelig ment udvalget,

at en selvstændig regulering får de lovgivningsmæssige hensyn bedre frem, som gør sig gældende ved datakriminalitet, udover de hensyn, som generelt gælder for formueforbrydelserne.
Nogle gerningsindhold vil i fremtiden kunne være omfattet af både almindelige bestemmelser og særlige databestemmelser, og i sådan et tilfælde kan begge bestemmelser bruges i konkurens. Et eksempel er ødelæggelse af data, som kan ske ved sletning eller ødelæggelse af det bærende medie eller ved et elektronisk indgreb. Begge tilfælde omfatter ødelæggelse af data og kan derfor være omfattet af den almindelige hærværksbestemmelse og den særlige datahærværksbestemmelse.
Ved en fremtidig regulering af bestemmelserne mod datakriminalitet, er det lettere overskueligt at samle bestemmelserne et sted. Da teknologien udvikler sig hurtigt, er det dog praktisk at lave bestemmelserne så brede og omfattende som muligt, dog med respekt for legalitetsprincippet.
Det foreslået kapitel omfatter kun de særlige handlinger mod datakriminalitet, mens anden kriminalitet, hvor datasystemer blot er et redskab, omfattes af de almindelige bestemmelser, som for eksempel krænkelse af privatliv ved offentlige ytringer.[49]

Det endelige resultat, som senere træder i kræft, er ikke helt som foreslået i 2007. Departementet er enig med udvalget i, at data i højere grad har behov for selvstændig beskyttelse, men mener ikke at IT-kriminalitet skal behandles anderledes end almindelig kriminalitet.
Departementet mente, at den foreslået ordlyd om datahærværk, i stedet for indsættes i den eksisterende hærværksbestemmelse.
I den eksisterende straffelov fra 1902, er hærværksbestemmelsen indsat i kapitel 28 om hærværk. I den nye straffelov fra 2005 oprettes et nyt kapitel 28 om hærværk og femkaldelse af fare for offentligheden. Dette kapitel indeholder udover hærværksbestemmelsen også bestemmelser om forsagelse af brand, oversvømmelse og lignende, som skader offentligheden samt den der fjerner redskaber eller på anden måde hindrer andre i at forebygge eller afværge ulykker.[50]

I 2004 blev hærværk mod data tilføjet til den almindelige hærværksbestemmelse i 1902-straffelovens § 291, og har nu den ordlyd, som 2005-straffelovens § 351 om hærværk vil få, når den endelige 2005-straffelov træder i kraft.

Modernisering af straffeloven sker igennem 3 dele, hvoraf den sidste del af denne modernisering lader vente på sig. Det er blandt andet bestemmelserne mod datakriminalitet der ikke er helt opdateret. Den gældende Straffelov omtales som 1902-straffeloven, selv om den almindelige del og halvdelen af den specielle del er resultatet af 2005-straffeloven.
Da Norge blev udsat for terror den 22. juli 2011, fandt man behov for flere ændringer i terrorlovgivningen. Dette skete med ændringslov nr. 85 af 21. juni. Loven styrkede kriminaliseringen og straffen for terror, men indeholdt også ændringer til 1902-straffeloven, som allerede var vedtaget. Disse ændringer skulle gælde fra, når 2005-straffeloven træder i kraft, men ændringer er med, for

[49] NOU nr. 2 fra 2007, pkt. 4.1.2
[50] Ot. prp. nr. 22 (2008-2009), pkt. 2.15.5.1

at sikre en tilstrækkelig dækkende straffelov, indtil den nye 2005-straffelov kan træde endeligt i kræft.
Ændringsloven tilføjer andet led til straffelovens § 291 om hærværk, således det klart fremgår af bestemmelsens 2. pkt., at den der ændrer, tilføjer, ødelægger, sletter eller skjuler andres data, straffes for hærværk.[51]
Den første handling, der kriminaliseres er ændring. Dette omfatter ændring af en enkelt fil, såsom en systemfil eller et word-dokument, men det kan også være en ændring i en database som for eksempel et kundekartotek. Den næste handling er ødelæggelse. Denne handling omfatter blandt andet den situation hvor gerningsmanden kryptere filer, så de ikke kan bruges af den berettigede. Sletter betyder af data fjernes. Handlingen omfatter enhver form for sletning, også selv om data kan genskabes. Skjule data, kan også betyde at kryptere data. Derudover kan gerningsmanden skjule en eller flere filer, ved at flytte dem til et andet sted på samme edb-system.
Det er samlet set ikke et krav, at skaden er uoprettelig. Selv om slettet data kan genskabes eller der forelægger en sikkerhedskopi af systemet, er gerningen stadig omfattet af bestemmelsen. Såfremt der er sket krænkelse af data, kan skadens omfang, blandt andet i lyset af en sikkerhedskopi eller muligheden for genskabelse, dog påvirke straffen til formidlende eller skærpende.[52]

5.3 Forslag til en dansk lovændring

Såfremt den uklare beskyttelse af data mod hærværk skal løses med en lovændring i Danmark, ligesom, Norge valgte at gøre, foreslås det at straffeloven suppleres med en ny bestemmelse, som i det følgende vil blive omtalt som § 291a. Bestemmelsen foreslås at se således ud:

> *"Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, som uberettiget ændrer, tilføjer, ødelægger, sletter eller skjuler en andens*
> 1) *oplysninger eller programmer, der er bestemt til at bruges i et informationssystem,*
> 2) *ikke-elektroniske oplysninger, der lagres på et fysisk medie.*
>
> *Stk. 2. Øves der hærværk af betydeligt omfang, eller af mere systematisk eller organiseret karakter, kan straffen stige til fængsel i 6 år"*

Ligeledes tilføjes § 291a i § 305, stk. 1 om påtalekompetencen, således den nye bestemmelse er underlagt samme påtaleregler som § 291.

[51] https://lovdata.no/dokument/NL/lov/1902-05-22-10 , 19. april 2015, kl. 01.00
[52] NOU nr. 2 fra 2007, pkt. 9.7

5.3.1 En ny bestemmelse

Som tidligere nævnt, overvejede udvalget i 2002 hvordan IT-kriminalitet skulle behandles. I den forbindelse kom man frem til, at hvor der skønnes et behov for specialbestemmelser, skulle disse indsættes i sammenhæng med den øvrige straffelov, da man ønskede at IT-kriminalitet så hvidt muligt skulle behandles som den øvrige kriminalitet.[53]
§ 291a, stk. 1, nr. 1 er lavet som et dansk eksempel svarende til den norske tilføjelse, mens stk. 1, nr. 2 går videre end det, og beskytter ikke-elektronisk lagret data også. Således sker der ikke en videre kriminalisering af elektronisk lagret data i forholdt til ikke-elektronisk lagret data.

5.3.2 Strafferammen

Den normale strafferamme er i stk. 1, og ligesom den almindelige hærværksbestemmelse er strafferammen bøde eller fængsel indtil 1 år og 6 måneder. Den forhøjet strafferamme i stk. 2 er ligeledes tilføjet på baggrund af den almindelige hærværksbestemmelse, som øger strafferammen indtil 6 års fængsel. Den forøgede strafferamme i § 291 blev ændret ved lov nr. 352, fra 19. maj 2004 i forbindelse med IT-kriminalitet, og er derfor videreført til denne bestemmelse.
Det er en konkret vurdering hvornår stk. 2 finder anvendelse. I U.1987.216Ø hvor data fik en afledt beskyttelse, blev skaden anset som betydelig på grund af den indgribende karakter og behovet for ekstern bistand. Skaden blev opgjort til 100.000 kr. for reetablering af data og for efterfølgende vedligeholdelse.
Når der nævnes systematisk eller organiseret karakter, er det endnu en konkret vurdering, men såfremt der er tale om kriminelle organisationer, taler det blandt andet for en skærpelse af straffen efter stk. 2.

På grund af udviklingen indenfor informationsteknologi, koster lagringsmedierne ikke ret meget i forhold til tidligere. I mange situationer kan de lagrede data for eksempel være en forretningshemmelighed, et testresultat eller lignende, og da har dataen ofte en større værdi for virksomheden end det bærende medie, som efter gældende ret er beskyttelsesobjektet.
Som det kommer til udtryk i dommen fra 1987, udmåles straffen ikke alene på baggrund af det bærende medies værdi, men på dets funktion og udgifter til genoprettelse af data.
Endelig lægger domstolen også vægt på sikkerhed og kontrol. Hvis der er mangel på sikkerhed og kontrol, som medfører opdagelsen af et eventuelt angreb kunne havde været mindsket, vil strafudmålingen blive mildere.[54]

5.3.3 Uberettiget

Handlingen skal være uberettiget, og som det kommer til udtryk i kommentaren til § 293, kan det følge af andre lovbestemmelser eller af en aftale, hvornår en handling er berettiget. Det er i sidste ende overladt til domstolen at afgøre om en handling er straffri, men fra andre områder, såsom brugstyveri, viser retspraksis at strafansvar kan være udelukket som følge af nære familiemæssige

[53] Betænkning nr. 1417 fra 2002, pkt. 2.4
[54] Betænkning nr. 1417 fra 2002, pkt. 2.3

relationer. Hvorvidt handlingen er uberettiget, kan også være vanskeligt at vurdere, når en medarbejder for eksempel ændrer eller sletter oplysninger om kunder i et kundekartoteket. I sådan et tilfælde må det være op til domstolen, at vurdere om der har været en tilstrækkelig klar aftale mellem arbejdsgiver og arbejdstager, til at kunne straffe medarbejderen.[55]

5.3.4 Ændrer, tilføjer, ødelægger, sletter eller skjuler

Den kriminelle handling minder meget om den, der er gældende for databedrageri efter § 279a. Ligesom handlingen efter § 279a kan være helt eller delvis, gælder det også for § 291a.[56] Yderligere straffer § 291a dog også for at ødelægge og for at skjule data, hvilket er inspireret af den norske bestemmelse.

Ødelæggelse kan virke overflødig, idet en tilføjelse, ændring eller sletning allerede omfatter de fleste handlinger, men ved at tilføje ødelæggelse, er alle tænkelige handlinger omfattet. Ødelæggelse kan således også bruges i stedet for tingsødelæggelse i § 291, hvor eksempelvis en magnet sletter data fra en harddisk. Dette er allerede beskyttet, men idet data i nogle situationer er mere beskyttelsesværdige end det bærende medie, vil gerningsindholdet hermed falde ind under § 291a i stedet for § 291. Dette vil blive nærmere behandlet i næste afsnit.

Skjule omfatter de situationer, hvor data ikke er påvirket, men hvor gerningsmanden eksempelvis har flyttet data på det bærende medie, så den berettigede ikke kan finde det. Det kan for eksempel være et dokument, som var lagret i mappen dokumenter, som uberettiget er flyttet til en skjult mappe, således dokumentet ikke kan hentes frem og dermed tjene sit formål.[57]

Situationen hvor data skjules for den, der har en berettiget adgang, minder om gerningsindholdet i § 293, stk. 2 om at hindre en anden i helt eller delvis at råde over ting, men denne bestemmelse omfatter som tidligere nævnt ikke data, da beskyttelsesobjektet også i den bestemmelse er ting.[58]

5.3.5 Oplysninger eller programmer, der er bestemt til at bruges i et informationssystem

Ordlyden svarer ikke til den norske bestemmelse, hvor man har valgt ordet data. I andre danske bestemmelser, såsom databedrageri og hackerbestemmelsen anvendes "oplysninger eller programmer, der er bestemt til at bruges i et informationssystem", og derfor er samme ordlyd valgt til § 291a.

Definitionen af denne ordlyd kommer til udtryk i kommentaren til § 263, stk. 2, hvor oplysninger er defineret som det samme som data. Data defineres som *"enhver form for repræsentation af kendsgerninger eller ideer, der kan kommunikeres eller behandles gennem en eller anden proces"*. Programmer er samme sted defineret som "*et sæt af specificerede kommandoer, der direkte eller indirekte styrer og sikrer gennemførelsen af en elektronisk databehandling"*.[59]

[55] Kommenteret straffelov – specielle del, side 598
[56] Kommenteret straffelov – specielle del, side 546
[57] NOU nr. 2 fra 2007, pkt. 9.7
[58] Kommenteret straffelov – specielle del, side 597
[59] Kommenteret straffelov – specielle del, side 442

Som det kom til udtryk i afsnittet om fortolkning, skal ordlyden så hvidt muligt fortolkes ens indenfor den samme lov. Sker der en ny fortolkning af ordlyden i § 263, stk. 2, vil denne fortolkning derfor også være gældende for § 291a, såvel som for § 279a om databedrageri.

5.3.6 ikke-elektroniske oplysninger, der lagres på et fysisk medie

Denne tilføjelse er lavet med inspiration fra persondatalovens § 1, stk. 2. Ved at tilføje ikke-elektronisk oplysninger, der lagres på et fysisk medie, sikres der en lige retsstilling mellem almindelig kriminalitet og IT-kriminalitet. De førnævnte overvejelser om at IT-kriminalitet skal behandles ligesom almindelig kriminalitet, må forudsættes at skulle gå begge vej.
Når oplysninger skal være en kombination af ikke-elektronisk og lagret på et fysisk medie, omfattes alle de nedskreven data og information, som tilhører en anden, i samme omfang som elektrisk lageret oplysninger og programmer.

5.4 Konsekvens ved en selvstændig beskyttelse

Når loven ændres, har det i nogle situationer både positive og negative konsekvenser. I dette afsnit vil nogle af disse konsekvenser derfor blive belyst.

5.4.1 Klarhed om hærværk af data

Som tidligere skrevet, er der ikke et klart svar på, om data selvstændigt er omfattet af hærværksbestemmelsen. Den foreslået tilføjelse til straffelovens § 291a giver en klarhed af reglerne, således praktikere af straffeloven og borgerne i retssamfundet ved hvad der er tilladt og hvad der er strafbart. Dette er netop hensigten med det strafferetlige legalitetsprincip.
Som det kom til udtryk i det tidligere afsnit om fortolkning af tingsbegrebet, kom det til udtryk at Inger Marie Sunde mener, at data bør være omfattet af hærværksbestemmelsen ud fra en formålsfortolkning. Hun gør ligeledes gældende, at det er et problem, såfremt ejeren af data ikke nyder samme beskyttelse, uanset om denne data er lagret på egne eller andres servere.
I forarbejderne i 1986 konkluderede man at data kun har en afledt beskyttelse. I 2002 kom man frem til samme resultat, dog med forbehold for at domstolen i en eventuel principiel sag om data, på baggrund af en fortolkning *kan* komme frem til at data alligevel er selvstændig beskyttet mod hærværk.
Både i Danmark og i Norge har man i mere end 30 år diskuteret om data er direkte eller indirekte omfattet af ting, og denne uvished bliver kun blevet større i kraft af den teknologiske udvikling.
Norge valgte netop med begrundelse i uklare regler, at tilføje data som selvstændigt beskyttelsesobjekt i den eksisterende hærværksbestemmelse.[60] Resultatet af denne løsning er at en tilstrækkelig klar beskyttelse af data er blevet sikret.
Problemstillingen minder den, der var gældende ved tilføjelsen af § 263, stk. 2, som også skete for at lave klare regler. Strafferetsrådet mente at det at det var muligt at § 263, stk. 1, eventuelt kunne fortolkes udvidende til også at omfatte informationer i et dataanlæg. Denne usikkerhed ønske-

[60] Ot. prp. nr. 22 (2008-2009) pkt. 2.15.5.1

de man ikke og tilføjede derfor § 263, stk. 2. Tilføjelsen præciserer at det er strafbart at skaffe sig uberettiget adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem. [61]

5.4.2 Konkurens og accessoriske forbrydelser

Når data nyder en selvstændig beskyttelse, sker der i nogle situationer at angreb på data er omfattet af flere straffebestemmelser på samme tid.

Det sker blandt andet når gerningsmanden sletter data fra en harddisk med en magnet, som dermed ødelægger systematikken i de magnetiske impulser, eller sætter ild til et ikke-elektronisk register. Med den eksisterende lovgivning, er denne ødelæggelse af data omfattet af den eksisterende hærværksbestemmelse, hvor data har en afledt beskyttelse. Lovændringen betyder at handlingen også kan være omfattet af § 291a. Det vil som udgangspunkt være uden betydning om § 291 eller § 291a anvendes, idet strafferammen er den samme, men det mest rigtige vil være at anvende § 291a, da dette gerningsindhold specielt beskytter data. Såfremt en senere lovændring skærper strafferammen for data eller flytter databeskyttelsen til en særlov, er det også særbestemmelsen der finder anvendelse.

Dette kommer blandt andet til udtryk ved de ophavsretlige regler. Et ophavsretligt beskyttet værk er ikke omfattet af § 291 når det gengives i en ødelagt udgave. Det er ikke tingen der beskyttes men derimod det ideelle værk. Værket er omfattet af de ophavsretlige regler i særlovgivningen, samt den overbyggende straffebestemmelse i straffelovens § 299b.

En anden situation er når ødelæggelsen er accessorisk forbundet med en alvorligere forbrydelse. Det kan for eksempel være når gerningsmanden skaffer sig uberettiget adgang efter § 263, stk. 2, for derefter at slette dataen. Denne situation kan sammenlignes med den gerningsmand der begår tyveri efter § 276 og samtidig beskadiger ting efter § 291. I sådan en situation straffes der normalt kun efter § 276, medmindre skaden er så stor, at det vil være mest rigtigt også at straffe for 291. Hvis der er tale om husfredskrænkelse efter § 264, stk. 1 efterfulgt af hærværk, straffes der både for husfredskrænkelse og hærværk for ødelæggelse af for eksempel fordøren. [62]

Det vil altså som udgangspunkt være § 291 a, der skal anvendes når data er angrebsobjektet. I tilfælde at uberettiget adgang efter 263, stk. 1 eller stk. 2 og ødelæggelse af data efter § 291a, vil der i de fleste tilfælde blive straffet efter § 263, alt efter ødelæggelsens omfang.

5.4.3 Anvendelsesområdet for hærværk

Når data beskyttes efter sin egen bestemmelse, kan man overveje om den almindelige hærværksbestemmelse begrænses i muligheden for en senere udvidet fortolkningen af ting. Konsekvensen heraf er, at uforudsete "ting" ikke nyder beskyttelse mod hærværk, og dermed stiger risikoen for frifindelse, på trods af en uønsket adfærd. Denne problemstilling er lig den, der netop bliver behandlet i dette speciale om data.

[61] Betænkning nr. 1032 fra 1985, side 23+78
[62] Kommenteret straffelov – specielle del, side 592

Når data ikke er omfattet af ting i § 291, kan det sammenlignes med de ideelle rettigheder over et ophavsretligt værk, som heller ikke er omfattet af hærværksbestemmelsen. Ophavsretlige værker beskyttes derimod igennem ophavsrettens kapitel 7, som straffer forsætlige og groft uagtsomme overtrædelser af flere opremsede bestemmeler i ophavsretsloven. Straf kan blandt andet pålægges den, der gør en andens værk tilgængeligt for offentligheden uden samtykke, jf. ophavsretsloven § 76, stk. 1, nr. 1. Derudover er der i straffeloven § 299b, en overbyggende bestemmelse til ophavsretslovens straffebestemmelse, som skærper straffen, når der forelægger særlig skærpende omstændigheder eller en uberettiget vinding. Denne straffebestemmelse gælder ikke kun for ophavsretlige værker, men for alle de immaterielle rettigheder.
Et maleri kan udsættes for hærværk, idet malleriet som en fysisk ting bliver ødelagt. Værket nyder altså en afledt beskyttelse af en fysisk ting, ligesom det er tilfældet for data efter gældende ret. Beskyttelsesobjekt er reelt rammen med lærredet. Værket, som kommer til udtryk på lærredet i rammen nyder en selvstændig beskyttelse igennem ophavsretsloven, og er altså ikke omfattet af ting. Det kan for eksempel være hvis værket gengives i en ødelagt udgave uden samtykke fra ophavsretsmanden.[63]
På samme måde vil data have en selvstændig beskyttelse, ved siden af den fysiske beskyttelse som data har nu. Den særskilte immaterielle beskyttelse illustrerer, at der er grænser for anvendelsen af begrebet ting, og denne afgrænsning har betydning for hvad der fremadrettet beskyttes, og hvad der kan kræve særskilt beskyttelse. Såfremt der opstår nye uforudsete situationer, som kræver beskyttelse af en ikke-håndgribelig ting, vil den særskilte beskyttelse af både ophavsretlige værker og immaterielle data tale imod en udvidet fortolkning af tingsbegrebet.

5.4.4 Cybercrime-konventionen

Cybercrime-konventionen stiller krav om en særskilt beskyttelse af data uafhængig af systemet. Det kommer til udtryk i konventionens kapitel 2, hvor der er en særskilt artikel til henholdsvis data og edb-system. Straffelovrådet fra 2002 tog konventionen i betragtning, da de gennemgik de eksisterende bestemmelser, og eftersom der ikke skete en direkte beskyttelse af data, taler det for at fortolke ting som data. Da det ikke klart kom til udtrykt i betænkningen, at data nyder direkte beskyttelse, vil en særskilt beskyttelse af data i en ny bestemmelse, give en utvivlsom tilstrækkelig beskyttelse af henholdsvis data og edb-system. På den måde er resultatet ikke kun en klar lovhjemmel, men også en klar implementeringen af cybercrime-konventionen materielle regler.[64]

5.5 Sammenfatning

I dette kapitel er specialet gået videre end at analysere gældende ret, til at foreslå en ny bestemmelse til straffeloven. Kapitlet starter med at undersøge, hvad der lå bag ændringen af den norske bestemmelse. På baggrund af den norske lovændring, og det foregående kapitel om analyse af

[63] Kommenteret straffelov – specielle del, side 592
[64] TfK.2013.240, pkt. 3.1.2

gældende ret, foreslås der i dette kapitel en selvstændig datahærværksbestemmelse til straffelovens kapitel 28 om formueforbrydelser.
Den nye bestemmelse beskytter både elektronisk og ikke-elektronisk lagret data, således IT-kriminalitet og almindelig kriminalitet nyder samme strafferetlig beskyttelse. Strafferammen i den almindelige hærværksbestemmelse og den ny er den samme, både den almindelige i stk. 1 og den skærpede i stk. 2. Ligeledes er påtalekompetencen den samme som i den almindelige hærværksbestemmelse, ved tilføjelsen af § 291a i forlængelse af § 290, stk. 1 og 3 i § 305. Det skyldes at den nye bestemmelse ikke skal ændre gældende ret, blot give mere klarhed over datahærværk.
I forlængelse med den nye bestemmelse, er konsekvensen af at tilføje en nye straffebestemmelse blevet gennemgået. Her er det blandt andet kommet til udtryk, hvordan reglerne blive mere klare, men også hvordan tingsbestemmelsen afgrænses i forbindelse med en senere usikker fortolkning.
Endelig opfylder den nye bestemmelse kravet i Cybercrime-konventionen om at beskytte data og edb-systemet særskilt, og der er derfor med den nye bestemmelse sket en klar implementering af konventionen.

6. KONKLUSSION

Dette speciale har haft til formål at undersøge hvordan data er beskyttet mod hærværk, og i den forbindelse om data er tilstrækkeligt beskyttet.

Interessen for dette speciale kommer sig af, at udviklingen indenfor informationsteknologi, har givet nye muligheder for privat- og erhvervslivet til at formidle information. Informationsbehandling er i sig selv ikke noget nyt, men teknologien har medført en ny verden af muligheder, og derfor er beskyttelsesbehovet vokset. Informationer er i højere grad blevet et formuegode, ligesom andre fysiske genstande, og har derfor behov for et tilstrækkeligt klart strafferetligt værn. Det strafferetlige værn skal beskytte information og de bagvedlæggende data mod tyveri, ødelæggelse og andre krænkelser, men dette speciale har afgrænset sig for den del, der går udover hærværk.

Det strafferetlige legalitetsprincip har til formål at sikre, at borgerne i retssamfundet kender sin ret. Borgeren skal have mulighed for at vide hvad der er tilladt og hvad der er strafbart. Med udgangspunkt i IT-kriminalitet, har dette speciale undersøgt hvorvidt data er tilstrækkeligt beskyttet af de gældende straffebestemmelser på baggrund af dette legalitetsprincip. Det fremgår ikke klart af ordlyden i den almindelige hærværksbestemmelse om data er beskyttet, idet hærværksbestemmelsen beskytter "en andens ting". Opgaven har derfor konkret været, at undersøge om data er en ting?

Data er et immaterielt formuegode, da en databehandling giver information, som kan give viden. Denne viden efterspørges i samfundet, og derfor er der opstået et stort marked for data. Dette marked bevirker at der ligesom for andre fysiske formuegoder, opstår et behov for en formueretlig regulering og en strafferetlig beskyttelse.
Hærværksbestemmelsens tingsbegreb er ifølge forarbejderne løsøre og fast ejendom. Det er dermed løsørebegrebet, der skal hjælpe til at vurdere om data er ting. Der blev i 1985 og i 2002 skrevet en betænkning, som undersøgte tingsbegrebet i forhold til data, men her blev data fortolket således, at data ikke i sig selv er en ting, men derimod nyder en afledt beskyttelse af de bærende medie, som opfylder kravet om at være en ting. I en dom fra 1987, skete der hærværk på information og programmer, og her fortolkede domstolen tingsbegrebet ligesom fortolkningen i betænkningerne.
Samlet set er gældende ret derfor, at data ikke i sig selv er beskyttet mod hærværk, men derimod nyder en afledt beskyttelse af systemet eller mediet som lagrer dataen.

På grund af den teknologiske udvikling, som skaber nye muligheder for lagring og transmission af data, opstår der situationer hvor den afledte beskyttelse ikke ud fra ordlyden er klart tilstrækkelig. Cloud computing er især et voksende område, som har til hensigt at overtage de ressourcer som både private og virksomheder bruger på lagringsplads. Udbyderne stiller således lagerplads til rådighed i det virtuelle rum, således dataen kan tilgås overalt, af den, der har en berettiget adgang. Denne løsning giver en masse frihed for den enkelte bruger, men i forhold til angreb på dataen, opstår der en tvivl om hvem der nyder den strafferetlige beskyttelse. Da hærværk beskytter en

andens ting, er det som udgangspunkt ejeren af tingen, altså serveren, der beskyttes. Da påtalekompetencen for hærværk er ved den forurettede, betyder det, at det således er udbyderen af lagerplads der er påtaleberettiget og ikke ejeren af den lagret data. Det er et problem, hvis udbyderen af lagerplads ikke ønsker at anmelde angrebet, som for eksempel kan skyldes en uønsket offentlig interesse i udbyderens datasikkerhed.

Derudover er fortolkningen om den afledte beskyttelse på grænsen af en korrekt implementering af Cybercrime-konventionen. Konventionen har en særskilt artikel mod henholdsvis data- og systemangreb. Ved en afledt beskyttelse, er det i sidste ende stadig systemet der er angrebsobjektet. Når der i betænkningen ikke er udelukket en udvidet fortolkning af ting, til også at omfatte data direkte i en principiel sag, er national ret ikke mangelfuld i forhold til konventionens materielle regler, men retsstillingen er dog uklar, så længe domstolen anvender den tidligere fortolkning.

I afsnittet om det strafferetlige legalitetsprincip, kom det til udtryk, at der er rum for fortolkning og i begrænset omfang også analogislutninger. Disse muligheder begrænses dog af, at fortolkningen ikke må gå videre, end det strafferetlige legalitetsprincippet stadig respekteres.
Ud fra en ordlydsfortolkning af det strafferetlige tingsbegreb, er det kommet til udtryk at tingsbegrebet generelt ikke omfatter information og dermed data. Fortolker man data udover strafferetten, kommer det til udtryk at data er omfattet af købeloven, som omfatter køb af løsøre. Ud fra en formålsfortolkning er der intet i vejen for at data kan være omfattet af ting, da formålet er at beskytte et formuegode. Strafferammen giver også rum til en bred fortolkning af ting, idet straffen er mild, da den strækker sig fra bøde til fængsel i 1 år og 6 måneder. En limitationsfortolkning afgrænser en bestemmelse i forhold til en anden. Hærværksbestemmelsen begrænses kun af ophavsretslovens beskyttelse af det ideelle værk, som også er et immaterielt formuegode. En generel selvstændig databeskyttelse afgrænses derfor ikke af de immaterielle regler.
Hvorvidt ordlyden kan strækkes til også at omfatte data er usikkert, men en vid fortolkning er ikke udelukket. Den eventuel senere vide fortolkning skal dog respektere legalitetsprincippet. Domstolen er ikke bundet af den tidligere fortolkning fra 1987, på trods af der stadig henvises hertil. Det betyder, som også kom til udtryk i betænkningen fra 2002, at domstolen i en principiel sag kan fortolke tingsbegrebet udvidende til også at omfatte data, og dermed skabe en klar retsstilling.

Lovgiver er tidligere stødt på situationer, hvor eksisterende bestemmelser skulle fortolkes, for at vurdere om den bedste løsning på en klar retsstilling er at lade domstolen fortolke udvidende, eller ændre og tilføje bestemmelser i straffeloven. Da IT-kriminaliteten blev vurderet i 1985, kom det til udtryk i betænkningen, at man overvejede hvorvidt freds- og ærekrænkelsesbestemmelserne § 263 og § 264, kunne finde anvendelse på en uberettiget adgang til et informationssystem. Man kom frem til, at § 263 kunne anvendes ud fra en vid fortolkning, men den bedste løsning var at tilføje hackerbestemmelsen i § 263, stk. 2. Således skirede man en tilstrækkelig klar hjemmel mod den nye IT-kriminalitet, som var på højde med de eksisterende bestemmelser om uberettiget adgang. Ligeledes sikrede man at det strafferetlige legalitetsprincip var opfyldt.

Ofte ser de nordiske lande på hinandens lovgivning, når nye bestemmelser skal udformes og eksisterende bestemmelser skal fortolkes. Det sker, fordi de nordiske lande, indenfor flere retsområder, har et sammenligneligt lovforarbejde og domstolspraksis. I dette speciale er den norske lovgivning inddraget, fordi Norge som det eneste nordiske land, har tilføjet data som et selvstændigt beskyttelsesobjekt i sin eksisterende hærværksbestemmelse. Det norske forarbejde til denne tilføjelse er derfor blevet undersøgt, for at finde baggrunden for, at Norge kom frem til en anden løsning end Danmark. I det norske forarbejde om tilføjelsen af data, fremgår det at overvejelserne omkring det norske genstandsbegreb er lig de danske overvejelser, og fortolkningen medførte samme resultat, som gav mulighed for en udvidet fortolkning.
Norge har arbejdet på en helt ny straffelov, og derfor overvejede man et selvstændigt kapitel for al IT-kriminalitet. Baggrunden for dette forslag var, at IT-kriminalitet rejser så mange spørgsmål til de enkelte gerningsindhold i de eksisterende bestemmelser, og derudover har mange begreber en selvstændig betydning indenfor IT-kriminalitet. Det medførte et forslag om en række nye bestemmelser. Det var ikke kun en datahærværksbestemmelse der blev foreslået som en særlig bestemmelse, men alle formueforbrydelserne blev foreslået i en yderligere datarelateret udgave. Da departementet skulle tage endelig stilling til dette forslag, besluttede man dog at IT-kriminalitet fortsat skulle behandles som almindelig kriminalitet, så vidt der er mulighed herfor. Departementet var dog enig i, at hærværksbestemmelsen ikke tilstrækkeligt klart omfattede data, og da behovet for at beskytte data ofte er større end behovet for at beskytte det bærende medie, tilføjede man den foreslået ordlyd til den eksisterende hærværksbestemmelse.

På baggrund af de overvejelser der var omkring hackerbestemmelsen og med inspiration fra norsk ret, har det været naturligt af overveje en lignende løsning, som sikrer data en tilstrækkeligt klar beskyttelse. I specialet er der derfor foreslået en dansk bestemmelse, i forlængelse af den eksisterende hærværksbestemmelse, som beskytter elektronisk og ikke-elektronisk lagret data. Formålet med denne bestemmelse er ligesom med § 263, stk. 2 og den norske tilføjelse, at give en klar beskyttelse af data mod hærværk. Med den nye bestemmelse vil der ikke være usikkerhed om, hvem der er forurettet, om de nationale forpligtelser er opfyldt, og om den afledte beskyttelse af data er tilstrækkelig, da data selvstændigt beskyttes mod angreb i den nye bestemmelse.
Når bestemmelsen går videre end den norske, er det fordi man fra lovgivers side har ønsket at IT-kriminalitet og almindelig kriminalitet skal behandles ens. Det må derfor gælde begge veje, når der foretages lovændringer i forbindelse med IT-kriminalitet.
I forlængelse af forslaget til en ny bestemmelse, er betydningen for den fremadrettet retsstilling blevet undersøgt. Da den nye bestemmelse ikke ændrer gældende ret, er det her kommet til udtryk, at konsekvensen blot er en tydeliggørelse af det strafferetlige værn mod datahærværk. Data får en selvstændig beskyttelse, således konventionen også tydeligt er implementeret. For at sikre en ens behandling af elektronisk lagret og ikke-elektronisk lagret data, omfatter bestemmelsen begge typer. Påtalekompetencen og strafferammen er den samme, uanset om angrebet sker mod en ting efter § 291 eller mod data efter § 291a.

Problemformuleringen stiller spørgsmålstegn ved, hvordan data er beskyttet mod hærværk, og om denne beskyttelse er tilstrækkelig.
Svaret på hvordan data er beskyttet er, ud fra en fortolkning af hærværksbestemmelsens, at tingsbegreb, nyder data en afledt beskyttelse af det bærende medie.

Den afledte beskyttelse af data udfordres af den teknologiske udvikling og samfundsudviklingen generelt. Hvorvidt den afledte beskyttelse er tilstrækkelig skal for det første besvares ud fra, om den gældende fortolkningen er tilstrækkelig. Fortolkningen begrænser databeskyttelsen, idet der er påvist eksempler på situationer, hvor data ikke nyde en tilstrækkelig klar tilknytning til et bærende medie. Da domstolen har mulighed for at lave en ny fortolkning, som giver data en særskilt beskyttelse, taler det for, at data nyder en tilstrækkelig beskyttelse.
Hvorvidt data er tilstrækkeligt beskyttet, må dog også besvaret ud fra det grundlæggende straferetlige legalitetsprincip, at straf kræver klar lovhjemmel. Da lovgiver tidligere har ændret og tilføjet i straffeloven, for at sikre en tilstrækkelig klar lovhjemmel, er den endelige konklusion, at forslaget om en ny bestemmelse med en klar ordlyd om databeskyttelse er at foretrække, så også data utvivlsomt nyder en selvstændig beskytte mod angreb.

7. ENGLISH SUMMARY

Data vandalism

This thesis is about the criminal protection of data against vandalism. Data itself is just numbers and characters, or a combination thereof, but after a data processing the data converts into valuable information. Based on the information, knowledge is created.
There is no difference in the value of the data when it is processed electronically or non-electronically, but in information technology development, a new world of opportunities has emerged. Opportunities for data collecting, data processing and communication. The possibilities are endless and the growing data industry, results in an increasing need for data protection against vandalism.

Under Danish law, it has been decided that IT crime should be treated under existing criminal laws, and in this context, data protection against vandalism has also been analyzed. The thesis is therefore based on electronically stored data, because the non-electronically stored data will be subject to the same penal treatment as long as possible of natural causes. Electronic data may after a data processing in a system, appear as both information, and applications that are intended to be used in an information system.

The regulation for vandalism is in the criminal law § 291 and it punishes the one who destroys another person's thing.
Since the understanding of the term "thing", from a well-known understanding means something physical and tangible, this thesis aims to analyze "thing" in § 291 in proportion to data. The task is to find out how data is protected by vandalism and subsequent evaluate if this protection is sufficient.

The analyze of the term "thing" seems to express that data has a deflected protection of the physical media which stores the data. This protection comes from an interpretation of the term "things", and is to a certain extent sufficient. When the stored data itself has a greater value than the carrying media and the technological development brings networking solutions that challenge secondary protection, has the term "things" been interpreted to find out if "things" also protects the data directly. Based on an interpretation of things in the regulation for vandalism, it must be concluded that data generally are given a sufficient protection against data vandalism. Because of the principle of legality, it was necessary to examine whether a new regulation for data vandalism will be a better option. Based on the principle of legality, which is a fundamental principle of the rule of law, the conclusion is that an independent regulation for data vandalism is preferable.
Therefore there has been proposed a new regulation for data vandalism, which will complement the existing regulation for vandalism, so both electronically, stored and non-electronically stored data is protected against data vandalism.
The consequence of a new regulation is a clear authority in law for the protection of data against vandalism, and the new regulation does not further alter existing law.

8. LITTERATURLISTE

8.1 Bøger

- Baumbach, Trine, 2008, Det strafferetlige legalitetsprincip, 1. Udgave, DJØF forlag
- Greve, Vagn m.fl., 2013, Kommenteret straffelov – almindelige del, 10. Udgave, DJØF forlag
- Greve, Vagn m.fl., 2012, Kommenteret straffelov – specielle del, 10. Udgave, DJØF forlag
- Greve, Vagn, edb-strafferet, 2. Udgave, DJØF forlag
- Langsted, Lars Bo m.fl., 2012, Internetretten, 2. Udgave, Ex Tuto Puplishing A/S
- Michelsen, Aage, 1991, Skatteret Erhvervsret – Greve, Vagn, Erhvervsspionage – i straffe-retlig belysning, 1. Udgave, FSRs Forlag 1991
- Nørgaard, Peter, 2013, Private straffesager, 1. Udgave, Karnov group
- Sunde, Inger Marie, 2006, Lov og rett i cyberspace, 1. Udgave, Fagbokforlaget Vigmostad & Bjørke AS
- Sunde, Inger Marie, 2010, Automatisert inndragning, Avhandling ved Oslo Universitet
- Udsen, Henrik, 2013, IT-retten, 1. Udgave, Ex Tuto Publishing A/S

8.2 Artikler

- Mathiasen, Peter Dueholm, 2013, Cloud computing og den strafferetlige beskyttelse af data, TfK.2013.240

8.3 Betænkninger o.l.

- Betænkning nr. 1485 fra 2006 - om forurettedes processuelle retsstilling i straffesager
- Betænkning nr. 1032 fra 1985 – Straffelovrådets betænkning om datakriminalitet
- Betænkning nr. 1417 fra 2002 – Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet
- Justitsministeriets vejledning nr. 224 af 15. Oktober 1969
- Norges offentlige utredninger nr. 2 fra 2007
- Norges offentlige utredninger nr. 31 fra 1985
- Odelstingsproposisjon 22 (2008-2009)

8.4 Internetsider

- Den Store Danske, opslag på ”data”, 12. april 2015, kl. 20.00
  http://www.denstoredanske.dk/It,_teknik_og_naturvidenskab/Informatik/Software,_programmering,_internet_og_webkommunikation/data
- Den Store Danske, opslag på ”viden”, 9. maj 2015, kl. 12.00
  http://www.denstoredanske.dk/Sprog,_religion_og_filosofi/Filosofi/Filosofiske_begreber_og_fagudtryk/viden
- DR.dk – ”Dine cookies på nettet er mange penge værd”
  http://www.dr.dk/Nyheder/Penge/2014/08/26/171526.htm

9. LOV- OG DOMSREGISTER

9.1 Love

- Lovbekendtgørelse nr. 871 fra 4. Juli 2014, Straffeloven
- Lovbekendtgørelse nr. 140 fra 17. Februar 2014, Købeloven
- Lovbekendtgørelse nr. 1216 fra 25. September 2013, Markedsføringsloven
- Ændringslov nr. 55 fra 2004 (om blandt andet markedsføringsloven § 10 og straffeloven § 301a)
- Lov-1902-05-22-10, Almindelige borgerlig Straffelov (1902-Straffeloven i Norge)
- Lov-2005-05-20-28, Almindelige borgerlig Straffelov (2005-Straffeloven i Norge)
- Cybercrime-konventionen

9.2 Domme

- Retten i Hjørring af 14. Januar 2013 – Hæleri
- U.2011.877V
- U.2011.539H
- SH.2003.P-0012-00
- U.2003.1907Ø
- U.2003.1950Ø
- TfK.2001.177/2
- U.1994.520/2H
- U.1996.356Ø
- Øster landsretsdom af 13. februar 1995 – Proms kemiske fabrikker
- U.1987.216Ø
- U.1985.315H
- U.1984.645V
- U.1965.535V
- U.1963.1029V
- U.1960.746/2