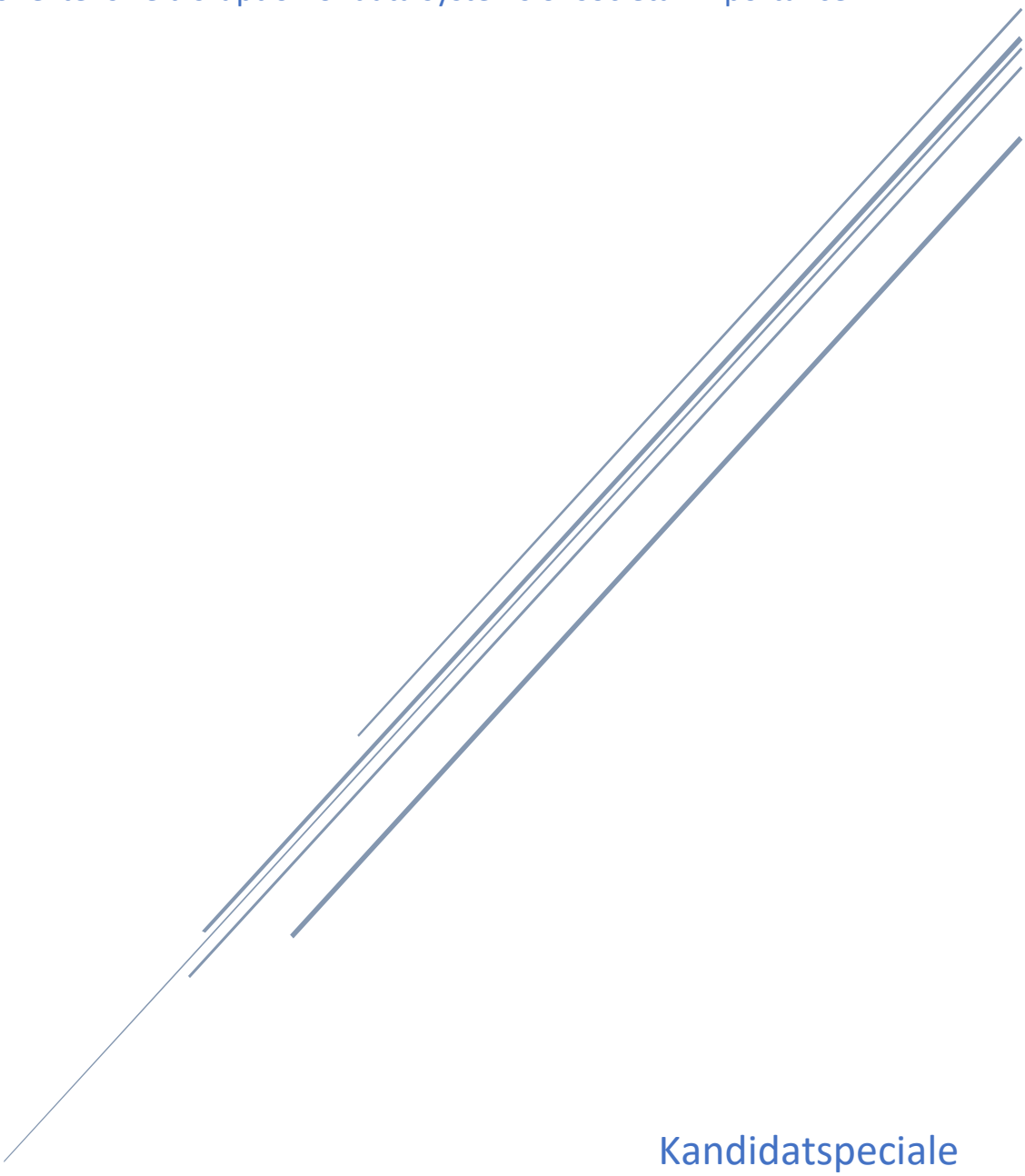
STRAFFELOVENS § 193, STK. 1

En analyse af omfattende forstyrrelse af samfundsvigtige data-systemer

The Danish Criminal Code section 193(1)

An analysis of extensive disruption of data systems of societal importance



Kandidatspeciale
Aalborg Universitet

Titelblad

Dansk tItel: Straffelovens § 193 - Omfattende forstyrrelse af samfundsvigtige datasystemer i et nutidigt perspektiv

Engelsk titel: The Danish Criminal Code section 193(1) – An analysis of extensive disruption of data systems of societal importance

Uddannelse: Jura, Aalborg Universitet

Projekt: Kandidatspeciale

Fagområde: Strafferet

Antal anslag: 115.021

Forfatter: David Ingemann van Rooij (studienummer: 20176708)

Vejleder: Lene Wacher Lentz

Afleveringsdato: 17. maj 2023

Abstract

The following project will focus on The Danish Criminal Code section 193 (1), which make it a criminal offence to cause an unlawful extensive disruption in the operation of ordinary means of transport, public postal services, telegraph or telephone installations, radio or television installations, socially important data systems or installations that serve for the general supply of water, gas, electricity, or heat.

To further restrict the focus of the project the main focus will revolve around the extensive disruption in the operation of socially important data systems.

The question that this project will seek to answer is what the terms “extensive disruption” and “socially important data systems” may include.

The overall method for the project will be the legal dogmatic method which seek to describe applicable law. In doing so the project will analyze the wording of The Danish Criminal Code section 193 (1), case law,

The project is divided into 7 chapters, which seek to further the understanding of the application of The Danish Criminal Code section 193 (1).

Chapter 1 will contain a short introduction to the project, a statement of the problem, the method used for the project, a delimitation of the project.

Chapter 2 contains a description of the relevant national and EU legislation that applies to the project.

Chapter 3 will contain an analysis of Section 193, subsection of the Criminal Code. 1, in which an interpretation of the provision will be included based on the law, legislative proceedings, reports and case law. The focus of the chapter will be to analyze in depth what can be derived from

expressing "unlawful solicitation", "data systems" and "extensive disturbance". At the end of the chapter, a summary will be made in the form of a partial conclusion.

In Chapter 4, a negative delineation will be made of The Danish Criminal Code Section 193 (1) in relation to selected legal rules. This is intended to illustrate and delineate how the considered criminal code for the project's focus area differs from comparable criminal codes.

Chapter 5 will contain an analysis of Section 193 (1) in accordance with The Danish Criminal Code Section 1 and the European Convention on Human Rights Article 7. This will be done to examine whether the provision in its current appearance is sufficiently clear in its wording and clarify whether this conflicts with the principle of legality. In this assessment case law by the European Court of Human Rights will be included.

Chapter 6 will contain an analysis of § 193 of the Criminal Code based on a comparative interpretation of the NIS directive. In this case, the NIS directive will be used as an interpretative contribution to the investigation of the scope of application of § 193 (1).

Chapter 7 will finally contain a conclusion of the project based on the other chapters. The project has concluded that even though the scope of section 193 (1) is rather vague in its current form The Danish Criminal Code section 193 (1) is clear enough that is does not conflict with the principle of legality of either The Danish Criminal Code section 1, or the European Convention on Human Rights Article 7. Furthermore it can be concluded that the definition of the term data systems has a far reaching field of application, but is stated in the provisions to Section 193(1), that application must be considered in conformity with the term extensive disturbance.

1.1 Indledning

I takt med den stigende digitalisering af samfundet og den stigende afhængighed af digitale systemer, er truslen mod angreb på datasystemer blevet en stadig større bekymring for mange.

Mange systemer er efterhånden styret af en eller anden form for digitalisering, hvorom dette er badevægte, biler eller større anlæg der har stor betydning for mange. Dette er både privatpersoner, private virksomheder og offentlige myndigheder. Cyberangreb på datasystemer kan have store konsekvenser for mange. Angrebene har gennem tiden antaget en mere sofistikeret karakter og det er derfor blevet nødvendigt at hav et effektivt lovgivningsmæssigt værktøj til at beskytte datasystemer mod angreb.

En sådan lov kan findes i form af f.eks. Straffelovens § 193, der kriminaliserer den retsstridige omfattende forstyrrelse af bl.a. samfundsvigtige datasystemer. Men hvad menes der egentlig i udtrykket ”samfundsvigtige datasystemer”? Og hvornår vil en forstyrrelse være ”omfattende”? Vil en hjemmeside såsom Facebook, YouTube eller Twitter være samfundsvigtigt eftersom at mange mennesker bruger disse tjenester til dagligt? Bestemmelsen kan i sin umiddelbare form virke intetsigende og det er derfor give anledning at dette projekt vil fokusere på netop denne bestemmelse i Straffeloven.

Dette leder derfor til nedenstående problemformulering.

1.2 Problemformulering:

”Formålet med denne afhandling er at analysere anvendelsesområdet af Straffelovens § 193, med særligt fokus på omfattende forstyrrelse af samfundsvigtige datasystemer med inddragelse af en nutidig forståelse heraf”

1.3 Afgrænsning

Centralt for denne afhandling er Straffelovens § 193, stk. 1, med særligt fokus og fortolkning af udtrykket ”samfundsvigtige datasystemer”. Straffelovens § 193, stk. 2, omhandler grov uagtsomhed og dette vil ikke blive yderligere behandlet i afhandlingen.

Straffelovens § 193 har været omdrejningspunkt for diskussion vedrørende ”ulovlige” arbejdsstrejker, hvori dette må resultere i driftsforstyrrelser, som følge af strejken. Det er i litteraturen et omdiskuteret emne, hvor der både argumenteres for og imod, at en ulovlig arbejdsstrejke vil være omfattet af bestemmelsen. Dette vil imidlertid ikke blive behandlet dybdegående i projektet.

Ydermere vil omfattende forstyrrelse af samfundsvigtige datasystemer kunne forekomme på mange måder, og på kryds af landegrænser, hvilket vil kunne opstille behandlingsspørgsmål vedrørende værneting. Dette vil ej heller blive behandlet i afhandlingen, da inkluderingen af værnetingsspørgsmål vil være for omfangsrigt til behandling i afhandlingen, og vil kunne grundlag for en afhandling i sig selv.

Udover Straffelovens § 193, stk. 1, vil §§ 263, 291, og 293 blive behandlet til belysning af anvendelsesområdet for § 193, stk. 1. Dette gøres for at sammenligne de udvalgte bestemmelser og undersøge om der er ligheder til anvendelsen, og dermed at disse kan bidrage til fortolkningen af straffelovens § 193.

NIS 2-direktivet blev i 2020 vedtaget i Europa-Parlamentet men er endnu ikke implementeret i dansk lov. Det vides derfor ikke *hvordan* eller i hvilken form denne vil blive implementeret, og ej heller, om denne vil implementeres i sin helhed. NIS 2-direktivet vil derfor på nuværende tidspunkt have lille fortolkningsværdi i forhold til projektet, og vil derfor ikke inddrages for dette projekt.

1.4 Metode

Dette speciale tager udgangspunkt i den retsdogmatiske metode, hvor gældende ret beskrives og analyseres (de lege lata), gennem en systematisk, metodisk og transparent virksomhed[1]. Fremstillingen af den retsdogmatiske metode vil komme til syne ved analyse af de individuelle elementer i Straffelovens § 193, stk. 1 hvortil de forskellige gerningsmomenter i bestemmelsen vil analyseres. Eftersom at den retsdogmatiske metode beskæftiger sig med gældende ret, er denne *ikke* løsningsorienteret i sin natur[2]. På den baggrund vil eventuelle uklarheder i den analyserende del blive redegjort for. Retskilderne i projektets analyse vil følge retskildehierarkiet og omfatte loven, lovforarbejder, retspraksis, høringsnotater samt juridisk litteratur.

I folkestyret er loven den højst vægtede retskilde da denne er fastlagt af Folketinget og vil derfor være forpligtende for henholdsvis myndigheder, erhvervsdrivende og borgere[3]. Loven vil derfor spille en stor rolle for projektets analyserende del. Som bidrag til lovfortolkningen vil lovforarbejder, betænkninger og bemærkninger inddrages. Disse er ikke selvstændige retskilder men kan inddrages til belysninger og bidrag til fortolkning af loven[4].

Ydermere har Danmark implementeret Europa-Parlamentets og Rådets Direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (Herefter NIS-direktivet), ved lov en række forskellige love som vil blive behandlet i projektet. Ved implementeringen af NIS-direktivet

Retspraksis anses som en retskilde ud fra en lighedsideologi hvor det lige skal behandles lige. På denne måde vil borgere kunne danne sig en formodning om, at tidligere afsagte domme vil danne en lige retsstilling for dem såvel som andre borgere[5]. Retspraksis vil i den henseende analyseres i forening med Straffelovens § 193, stk. 1 til illustration af hvilke overvejelser domstolene gør sig i forbindelse med anvendelsesområdet og fortolkning af bestemmelsen. Inden for domstolene

[1] Munk-Hansen – Retsvidenskabsteori 2. udgave, s. 204
[2] Munk-Hansen – Retsvidenskabsteori 2. udgave s. 204
[3] Bryde Andersen – Ret og metode 1. udgave, s 133 og Dorte Høilund – Retssikkerhed og juridisk metode, 2. udg., side 23
[4] Munk-Hansen – Retsvidenskabsteori 2. udgave, s. 261
[5] Munk Hansen – Retsvidenskabsteori 2. udgave, s. 315-316

findes såvel også en rangorden hvori dommes præjudikatværdi er stigende alt efter hvilken instans der har truffet afgørelsen. Således har højesteretsdomme større retskildeværdi end landsretsdomme, og landsretsdomme har større retskildeværdi end byretsdomme[6].

Den udvalgte retspraksis er fundet gennem Karnovs domsdatabase[7]. Det har ikke været muligt at få aktindsigt i den behandlede sag fra Retten i Roskilde af den 19. december 1996, hvorfor domsreferat, sagens anbringender, forhold og afgørelse har måtte findes i bet. 2002/1417 hvori dommen er gennemgået.

Juridisk litteratur anses ikke som en retskilde, da forfatteren savner legitimitet til at fastlægge ret[8]. Den juridiske litteratur kan dog med forbehold anvendes som supplerende bidrag til den teoretiske opfattelse af et retsområde samt en given retsstilling. Juridisk litteratur vil derfor anvendes hvor det findes relevant til at understøtte eller bidrage til forståelsen af gældende ret.

2. Lovgivningen

Fokus for dette projekt vil være på Straffelovens § 193, stk. 1. navnlig med særlig fokus på anvendelsesområdet og strafbarheden af betegnelsen ”omfattende forstyrrelse” og ”samfundsvigtige datasystemer”. Det er i den anledning relevant af danne et overblik over både den nationale lovgivning og det EU-retlige retsgrundlag.

2.1 Dansk lovgivning

Straffelovens § 193 har været genstand for en række revisioner siden den borgerlige straffelov af 1930, er det relevant at undersøge og fortolke forarbejderne til bestemmelsen.

Straffelovens § 193, stk. 1 har herefter gennemgået yderligere behandlinger og ændringer, navnlig med ændringen af lov nr. 229 af d. 06.06.1985 hvori ”databehandlingsanlæg” blev tilføjet til bestemmelsen. Herefter foretoges endnu en ændring af ordlyden ved lov nr. 352 af d. 19.05.2004, hvori betegnelsen databehandlingsanlæg blev ændret til ”informationssystemer”[9], for herefter

[6] Dorte Højlund – Retssikkerhed og juridisk metode, 2. udg., side 60-61
[7] Karnov.dk
[8] Munk-Hansen – Retsvidenskabsteori 2. udgave, s. 372-373
[9] Lov 352 af den 19.05.2004

igen at blive revideret ved lov nr. 1719 af d. 27.12.2018 som den seneste revision. Ved lov nr. 1719 af den 27.12.2018 blev ordlyden af bestemmelsen ændret til at omfatte "samfundsvigtige datasystemer" fremfor "informationssystemer"[10].

2.2 EU-retlig lovgivning

Den 24. februar 2005 vedtog Rådet for Den Europæiske Union rammeafgørelse 2005/222/RIA om angreb på informationssystemer. Formålet med rammeafgørelsen var at forbedre samarbejdet mellem de retlige og andre kompetente myndigheder, samt at foretage en indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler vedrørende angreb på informationssystemer.[11]
Danmark har implementeret Rådets rammeafgørelse 2005/222/RIA i dansk ret ved lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.).[12] Danmark har mulighed for at gennemføre regler svarende til direktivet, da direktivet ikke indeholder regler om gensidig anerkendelse.

2.3 Cybercrime-direktivet

I 2009 vedtog EU-medlemslandene Stockholm-programmet, hvori det blev anført at internettet havde skabt udfordringer i form af IT-kriminalitet, og at det derfor søgtes at EU burde fremme politikker og lovgivning som ville højne beskyttelsesniveauet. Dette beroede på øgede bekymringer om angreb på informationssystemer, især som led i organiseret kriminalitet, samt mulige terrorangreb på informationssystemer, der udgjorde en del af medlemsstaternes kritiske infrastruktur.

Kommissionen fremsatte d. 30. september 2010 et direktivforslag om angreb på informationssystemer, hvormed formålet var yderligere at sikre medlemsstaternes lovgivning i forhold til rammeafgørelse 2005/222/RIA. Dette direktiv blev vedtaget af Europa-Parlamentet og Rådet d. 12. august 2013, som direktiv 2013/40/EU om angreb på informationssystemer og om erstatning Rådets rammeafgørelse 2005/222/RIA (Cybercrime direktivet).[13]

[10] Lov 1719 af den 27.12.2018
[11] Rådets rammeafgørelse 2005/222/RIA, pkt. 1.
[12] Notat om tilvalg af cybercrime-direktivet, s. 1.
[13] Notat om tilvalg af cybercrime-direktivet, s. 1

Direktivet er vedtaget med henvisning til Traktatens art. 83, stk. 1, og er dermed omfattet af retsforbeholdet. Danmark deltog således *ikke* i vedtagelsen af direktivet og Danmark er dermed heller ikke bundet af direktivet, hvorom dette heller ikke finder anvendelse i Danmark.
Direktiv 2013/40/EU erstatter således Rådets rammeafgørelse 2005/222/RIA for de medlemsstater der har deltaget i vedtagelsen af direktivet.

3. Straffelovens § 193, stk. 1.

Straffelovens § 193 er placeret som den første bestemmelse i Straffelovens kapitel 21 omhandlende forskellige almenskadelige handlinger. Bestemmelsen kriminaliserer *"Den, der på retsstridig måde fremkalder omfattende forstyrrelse i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, samfundsvigtige datasystemer eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme, straffes med bøde eller fængsel indtil 6 år"*[14] jf. Straffelovens § 193, stk. 1.

Bestemmelsens ordlyd giver en række betingelser for fuldbyrdelsen at den strafbare handling i Straffelovens § 193, stk. 1 som skal være opfyldt før gerningsindholdet, vil være opfyldt. Herfra kan udledes, at der 1) skal foreligge en forstyrrelse. 2) forstyrrelsen skal være omfattende. 3) systemet og/eller anlægget skal være omfattet af bestemmelsen – altså bl.a. et samfundsvigtigt datasystem. 4) Forstyrrelsen skal være retsstridigt fremkaldt.

I lyset af projektets fokusområde giver bestemmelsen i sig selv anledning til en række spørgsmål som vil blive undersøgt og analyseret i afsnit 3.1-3.3, navnlig; hvornår er en forstyrrelse "retsstridig" fremkaldt? Hvad omfatter betegnelsen "datasystemer"? Hvornår vil sådanne datasystemer blive anset som værende "samfundsvigtige"? Hvornår vil en forstyrrelse blive anset som værende omfattende?

[14] LBKG 2022-09-28 nr. 1360 Straffeloven

3.1 Retsstridig fremkaldelse

Straffelovens § 193 har siden den borgerlige Straffelov af 1930 haft ordene "Den, der på retsstridig måde". Denne formulering angiver med ordene, at det ikke vil være enhver omfattende forstyrrelse af de anlæg der fremgår af bestemmelsen, der er strafbare. Formuleringen er dog ikke udelukkende gældende for Straffelovens § 193, da denne formulering går igen i andre bestemmelser i Straffeloven.

Det er med dette forbehold i lovteksten vedrørende den retsstridige måde et udtryk for, at det ikke har været muligt helt konkret af kvalificere det forhold som er søgt kriminaliseret, fra andre hyppigt forekommende forhold uden for den type af kriminelle type. Det er på den baggrund op til domstolene selv at vurdere, om en handling bør omfattes at gerningsbeskrivelsen i bestemmelsen. Dette vil skulle ske på baggrund af lovens motiver eller andre fortolkningsbidrag som vil kunne fremme forståelsen, og dermed også ligge til grund for om en handling har været retsstridig, og i så fald om der skal pålægges straf.

Det er i betænkninger til Straffelovens § 193 (daværende § 177) gjort tanker om begrebet retsstridighed, hvori indføjelsen af dette begreb beror på en overvejelse om ulovlige arbejdsnedlæggelser eller strejker kan anses som retsstridige.[15]. Hvis en ulovlig arbejdsnedlæggelse eller strejke forårsager en omfattende forstyrrelse i driften af de oplistede anlæg, må samfundet kunne søge beskyttelse ved anvendelse af straf. Der er dog eksplicit taget afstand fra at behandle dette spørgsmål fyldestgørende i betænkningen, da det både fra lovgivers og Straffelovrådets side ikke har været et ønske om, at gøre arbejdsstandsninger strafbare, da et sådant mellemværende vil bero på at lønkampe mellem organisationer skal kunne udkæmpes uden strafferetlig indblanding[16].

Det fremgår dog af den juridiske litteratur, at *"for så vidt angår ulovlige strejker kan § 193 vanskeligt tænkes anvendelig på de driftsforstyrrelser der direkte følger af ansattes arbejdsvægring"*[17].

Dette vil dog ikke yderligere søges behandles i afhandlingen, da fokus for denne netop omhandler omfattende forstyrrelse af samfundsvigtige datasystemer, selvom det kan tænkes, at ovenstående også gør sig gældende for datasystemer.

[15] Betænkning af 1923, s. 296.
[16] Betænkning af 1923, s. 296.
[17] Knud Waaben; Strafferettens specielle del, 6. reviderede udgave, s. 222

3.1.2 Forsøg og forsæt

Straffelovens § 193 kriminaliserer den groft uagtsomme eller forsætlige[18] "omfattende forstyrrelse i driften […]". Med dette in mente vil det ikke være nok at gerningspersonen har vurderet at forstyrrelsen vil være omfattende, men at personen har haft *forsæt* til, at forstyrrelsen anses som *værende* omfattende.[19]

I retspraksis henvises til en dom fra Vestre Landsret, hvori forsøgs- og forsætspørgsmålet behandles. I sagen havde tiltalte, under flyvningen ombord på et passagerfly, udtalt at have en pistol liggende i sin jakke eller lignende[20]. Tiltalte blev principalt tiltalt for overtrædelse af for omfattende forstyrrelse i trafikken af almindelige samfærdselsmidler jf. Straffelovens § 193, stk. 1, med subsidiær påstand om overtrædelse af Straffelovens § 193, stk. 1, jf. § 21, stk. 1.

Byretten lagde til grund i sin vurdering, at tiltalte måtte have indset at dennes udtalelse kunne have betydelig indvirkning på flyets videre flyvning, idet at besætningen af hensyn til passagerernes sikkerhed måtte reagere forskriftsmæssigt på baggrund af udtalelsen fra tiltalte, som ville medføre en ekstraordinær landing af flyet med omfattende forstyrrelse til følge[21]. Tiltalte fandtes på den baggrund at have haft *forsæt* til overtrædelse af Straffelovens § 193, stk. 1. Det anføres dog i den forbindelse, at udtalelsen fra tiltalte *ikke* forårsagede en egentlig og faktisk omfattende forstyrrelse, da tiltalte forholdt sig tavs, og ikke reagerede på flypersonalets henvendelser omkring forholdet, før landingen af flyet ved dens planlagte destination. Byretten fandt således at tiltalte alene ville kunne dømmes for forsøg på overtrædelse af Straffelovens § 193, stk. 1. jf. § 21, stk. 1[22]. Da sagen blev bragt for Landsretten ændrede Anklagemyndigheden dermed tiltalen for Landsretten fra *"at have fremkaldt […]"* omfattende forstyrrelse, til *"at have forsøgt at fremkalde […]"*. Landsretten skulle i den forbindelse udelukkende tage stilling til, om tiltalte kunne dømmes for forsøg på overtrædelse af Straffelovens § 193, stk. 1, jf. § 21, stk. 1.

[18] Knud Waaben; Strafferettens specielle del, 6. reviderede udgave, s. 222.
[19] Thomas Elholm m.fl.; Kommenteret straffelov speciel del, 12. udgave, s. 364
[20] U.2002.2700 V
[21] U.2002.2700 V
[22] U.2002.2700 V

Det blev under vidneforklaringerne i Landsretten forklaret, at fra tiltaltes side var tale om spøg i forbindelse med bemærkningen om pistolen i jakken, hvorimod forurettedes vidneforklaringer fastholdt, at tiltaltes stemmeføring og ageren ikke gav anledning til at opfatte situationen som så. Piloten havde under flyvningen ydermere overvejet muligheden for at nødlande flyet, men måtte konstaterende afslå muligheden, grundet at flyets landingsvægt var for stor grundet mængden af brændstof. Det fandtes i lyset af bevisførelsen i Landsretten, at tiltalte *ikke* havde forsæt til at forsøge at fremkalde en omfattende forstyrrelse i driften af almindelige samfærdselsmidler jf. Straffelovens § 193, stk. 1.[23]

Det illustreres i dommen, at selvom tiltaltes bemærkning var grundlag for en potentiel omfattende forstyrrelse i driften, i form af pilotens overvejelser og muligheder for en nødlanding, var dette imidlertid ikke nok til at realisere hverken forsæt eller forsøg på overtrædelse af Straffelovens § 193. Det er så at sige ikke følgevirkningerne af gerningspersonens handlinger som må lægges til grund ved forsætspørgsmålet, men derimod om gerningens tilsigtede udfald har været en omfattende forstyrrelse, om det være forsøg eller forsætligt. Det er på den baggrund en konkret betingelse for bestemmelsens anvendelse, at den omfattende forstyrrelse skal være realiseret og ikke blot være potentiel.
Dette leder endvidere til spørgsmålet om hvordan fremkaldelsen af forstyrrelsen skal være fremkaldt når der er tale om et datasystem.

3.1.3 Retsstridig fremkaldelse ved datasystemer

Forstyrrelsen af datasystemer vil efter lovforarbejderne kun opnå strafferetlig beskyttelse hvis der er tale om angreb der helt lammer eller i betydeligt omfang forstyrrer registrering, behandling og transmission af data[24]. Denne type angreb vil hyppigst forekomme i form af f.eks. Denial-of-Service (DoS-angreb), distributed denial-of-service (DDoS-angreb), Malware eller ransomware.
DoS-, og DDoS-angreb hindrer brugen af et system ved at overbelaste systemerne til et punkt hvor systemet bryder sammen. Dette sker oftest ved brug af Internet Protokol-pakker der sendes i massive mængder, således at systemet ikke kan sende eller modtage andre former for information[25].

[23] U 2002.2007 V
[24] LFF 2018-10-03 nr. 20 Ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (freds- og ærekrænkelser m.v.), bemærkning til nr. 3.
[25] Jan Trzaskowski mfl., Internetretten, s. 604

Den tilsigtede virkning er dermed en rådighedshindring til systemet om det være sig delvist eller fuldstændigt og midlertidigt eller på ubestemt tid[26]. Malware er generelt set en samlebetegnelse for vira, orme, trojanske heste, keyloggere osv. Hovedformålet med malware er enten at angribe fortroligheden, integriteten, eller tilgængeligheden på et system. Virusser gør skadelige eller uønskede ting på de computere eller systemer som de inficerer uden ejerens viden eller samtykke hertil som f.eks. sletning af data eller programfiler.
En orm er malware, som spreder sig fra maskine til maskine, i form af et selvstændigt program. Ormen vil oftest have en skadelig last (payload) i form af virus eller en trojansk hest. En trojansk hest er malware som umiddelbart ser harmløs ud, men bruges til at fjernstyre offerets computer. Yderligere kan installeringen af en trojansk hest give afsenderen mulighed for selv at installere en bagdør i et system. På denne måde vil adgangen bruges til at foretage et DoS-angreb mod andre tilknyttede systemer[27].
Sidst men ikke mindst er ransomware, som er en virus, der har til formål at kryptere brugerens data. Herefter vil brugeren få besked om, at brugeren kan få nøglen til afkodning af sine data, hvis der udbetales en løsesum[28].

Fælles for de ovenstående typer angreb er, at brugeren mister rådigheden over systemet, da denne afskæres enten ved nedbrud, ødelæggelse eller konkret fratagelse af rådigheden. Det er derfor vigtigt at have for øje, at lovforarbejderne omfatter angreb, om disse er berigelsesforbrydelser i form af ransomware, eller anden form for angreb, der har til sigte at påvirke rådigheden til systemet.

3.2 Datasystemer

Begrebet ”datasystemer” blev tilføjet til Straffelovens § 193, stk. 1, ved lov nr. 1719 af 2018 og substituerede det daværende begreb ”informationssystemer”, som ligeledes blev indsat i stedet for begrebet ”databehandlingsanlæg”[29]. Ordlyden i bestemmelsen har været udsat for to ændringer siden tilføjelsen af ”databehandlingsanlæg” i 1985, og der er derfor relevant, at undersøge om

[26] Jan Trzaskowski mfl., Internetretten, s. 604
[27] Jan Trzaskowski mfl., Internetretten, s. 606
[28] Jan Trzaskowski mfl., Internetretten, s. 606
[29] Henholdsvis L 2018-12-27 nr. 1719, L 2004-05-19 nr. 352 og L 1985-06-06 nr. 229.

udviklingen i udtrykkene har haft betydning for anvendelsesområdet for Straffelovens § 193, stk. 1.

Databehandlingsanlæg blev tilføjet til Straffelovens § 193, stk. 1 ved lov nr. 229 af d. 06.06.1985. Det blev af Straffelovrådet påpeget at bestemmelsen, inden tilføjelsen af databehandlingsanlæg, ikke indeholdt nogen begrænsninger med hensyn til de anvendte midler hvorom en forstyrrelse i driften kunne antage. Hertil blev yderligere anført at "omfattende forstyrrelse på de i § 193 nævnte områder kan forvoldes ved et uretmæssigt indgreb i datastyring af bl.a. jernbanedrift eller luftfart eller i de af dataanlæg benyttede transmissionsledninger m.v., for så vidt disse kan betegnes som "almindeligt benyttede telegraf- eller telefonanlæg"".[30] Omvendt kunne tænkes angreb med omfattende forstyrrelse til følge, som bestemmelsen i sin daværende fremsætning ikke kunne henføre under bestemmelsen, medmindre der gjordes brug af en analog fortolkning af Straffelovens § 193[31]. Dette beroede på en vurdering af, at skadevirkningen ved angreb på databehandlingsanlæg potentielt kunne medføre omfattende forstyrrelser af væsentlige samfundsfunktioner[32]. Det blev således yderligere anført, at der ikke ville blive stillet krav til hverken størrelsen eller karakteren af de dataanlæg som var omfattet af bestemmelsen, da kravet om at forstyrrelsen i driften måtte være omfattende var begrænsende nok, for anvendelsesområdet for bestemmelsen[33]. Om omfattende forstyrrelse se afsnit 3.3.

Ved indføjelsen af "informationssystemer" i Straffelovens § 193, stk. 1 ved lov nr. 352 af d. 19.05.2004 blev der på baggrund af forarbejderne til lov nr. 229 af d. 06.06.1985 ikke gjort store forsøg på at afgrænse hvilke informationssystemer som måtte være omfattet af bestemmelsen, og der blev i derimod blot henvist til Straffelovrådets betænkning nr. 1032/1985 hvortil det igen blev anført, at bestemmelsen var tilstrækkeligt begrænset i sit anvendelsesområde i relation til databehandlingsanlæg (og informationssystemer), da anvendelsen ville afhænge af, at der var foretaget en omfattende forstyrrelse i driften. Det fremgik dog at der var et ønske om, at der med tilføjelsen

[30] Betænkning nr. 1032/1985, s. 41
[31] Betænkning nr. 1032/1985, s. 41
[32] Betænkning nr. 1032/1985, s. 41
[33] Betænkning nr. 1032/1985, s. 77

af informationssystemer blev søgt et mere neutralt begreb i forhold til mulige teknologiske løsninger.[34]

Ved lov nr. 1719 af d. 27.12.2018 blev "samfundsvigtige datasystemer" indføjet i Straffelovens § 193, stk. 1. Ved betænkning nr. 1563/2017[35] blev der gjort tanker om udtrykket "informationssystemer", samt dennes plads i Straffeloven som ledte til at udtrykket blev udskiftet med "samfundsvigtige datasystemer". Idéen med anvendelsen af udtrykket "informationssystem" i stedet for det tidligere anvendte "anlæg til elektronisk databehandling", valgte man dette udtryk grundet dens neutralitet i forhold til mulige teknologiske løsninger[36]. Endvidere blev der anført, at udtrykket "informationssystem" som ordbogsdefinition var snævrere end hvad der ligger i straffelovens brug af udtrykket, samt at udtrykket i sin natur blot vil vedrøre et system til behandling af information. Udtrykket ville ud fra en ordlydsfortolkning dermed række bredere end hvad Straffeloven tilsigtede, da det ifølge ordlyden, ikke var et krav om at behandlingen skulle ske ved hjælp af en maskine[37].
I de videre overvejelser gjorde Straffelovrådet sig tanker om der burde skæves eller til dels følge terminologien i Rådets rammeafgørelse 2005/222/RIA om angreb på informationssystemer. Rammeafgørelse 2005/222/RIA definerer et "informationssystem" som værende *"enhver enhed eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af edb-data samt edb-data, som lagres, behandles, fremfindes eller overføres i forbindelse med systemernes drift, brug, beskyttelse og vedligeholdelse"*[38] jf. art. 1, litra a.
Derudover skæves der også til art. 2, litra a, i Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 (cybercrimedirektivet), som har tæt på en identisk definition af informationssystem som Rådets rammeafgørelse 2005/222/RIA. Hertil holdes yderligere for øje, at "edb-data" defineres som *"enhver form for gengivelse af fakta, informationer eller begreber i et format, der egner sig til behandling i et informationssystem, herunder et program, som kan anvendes til at få*

[34] FT 2003-04 Tillæg A, s. 1793
[35] Betænkning nr. 1563/2017
[36] LFF 2003-11-05 nr. 55, pkt. 2.2.1.1
[37] Betænkning nr. 1563/2017, s. 57
[38] Rådets rammeafgørelse 2005/222/RIA af 24-02-2005

et informationssystem til at udføre en funktion" jf. rammeafgørelse 2005/222/RIA art. 1, litra b, samt cybercrimedirektivets art. 2, litra b.
Disse to definitioner af henholdsvis "informationssystem" og "edb-data" er så at sige uløselige, da definitionen af informationssystem indeholder edb-data som definitionsbidrag, og edb-data er defineret efter at disse egner sig til behandling i et informationssystem.[39]

Det blev endvidere overvejet i Straffelovrådets betænkning, at udtrykket "enhed eller anlæg til automatisk databehandling" skulle træde i stedet for "informationssystem", da det på den baggrund både ville omfatte anlæg i den forstand som fremgik af det tidligere anvendte udtryk "databehandlingsanlæg" samtidig med, at udtrykket "enhed" ville afspejle den automatiske databehandling som foregår på helt små enheder som foregår i dag. Udtrykket "automatisk" ville sikre sproglig dækning for automatiserede databehandlingssystemer, der eventuelt anvender ikke-elektronisk teknologi[40]. Denne formulering blev dog hurtigt opgivet, da et så langt udtryk ville føre til tunge og lange sætningskonstruktioner. Yderligere lagde Straffelovrådet til grund, at udtrykket "informationssystem" ikke har givet anledning til afgræsningsvanskeligheder eller andre problemer i praksis, samt at det heller ikke anses for nødvendigt at anvende udførligt udtryk i loven når et mere entydigt og præcist udtryk var tilstrækkeligt[41]. Dette kan imidlertid også fremstå betænkeligt, da det i den særdeles begrænsede litteratur vedrørende Straffelovens § 193, er anfægtet, at der netop ved anvendelsen af udtrykket "informationssystem" har måtte være grobund for fortolkningsbesvær ved domstolene[42].

I takt med den eksplosive integrering af datasystemer i flere og flere anlæg og hverdagsgenstande vil det synes overhængende, at finde ud af hvad der fra lovgivers side er ment med udtrykket "datasystemer".
Begrebet "datasystem" blev, tilføjet til Straffelovens § 193, stk. 1, ved lov nr. 1719 af 2018 og substituerede det daværende begreb "informationssystemer", som ligeledes blev indsat i stedet for begrebet "databehandlingsanlæg". Som beskrevet i det ovenstående, blev informationssystem

[39] Betænkning nr. 1563/2017, s. 58
[40] Betænkning nr. 1563/2017, s. 58
[41] Betænkning nr. 1563/2017, s. 59
[42] Helena Lybæk Gudmundsdottir Juristen. 3, s. 107-113

tilføjet, da det var neutralt til mulige teknologiske løsninger[43]. Forarbejderne til lovændringen i 2004 hvori informationssystemer indgik fremgår det at der *"Ved et informationssystem forstås en computer eller andet databehandlingsanlæg. Omfattet heraf er navnlig personlige computere, herunder både stationære og bærbare computere. Også andet elektronisk udstyr vil imidlertid kunne være omfattet, hvis udstyret har funktioner svarende til dem, der findes i computere. Det gælder således elektronisk udstyr, der kan anvendes til at oprette og/eller behandle dokumenter, billeder eller lyde, udføre regnskabsfunktioner og lignende, herunder også hvis sådanne funktioner senere forekommer i kombination med andet elektronisk udstyr, f.eks. fjernsyn."*[44]
Begrebet "datasystem" skal forstås i forenelighed med det dagældende informationssystem, med revideringen af Straffelovens § 193 ved lov nr. 229 af den 06.06.1985 blev implementeringen af strafferetlige værn mod datakriminalitet indføjet. Ved indføjelsen blev begrebet "databehandlingsanlæg" tilføjet hvortil det søgtes at beskytte denne type anlæg.

Ydermere vil databehandlingsanlæg, computere og andet elektronisk udstyr være omfattet, hvis dette har funktioner svarende til dem, der f.eks. findes i tablets og smartphones. Derudover vil elektronisk udstyr der kan anvendes til at behandle og oprette dokumenter, billeder, lyde, udføre regnskabsfunktioner og lignende, herunder også hvis disse funktioner senere forekommer i kombination med andet elektronisk udstyr[45]. Dette står i kontrast til de andre ellers objektivt omfattede anlæg, som fremgår af bestemmelsens ordlyd, hvor domstolene må tillægge dette stor betydning i bedømmelsen af bestemmelsens anvendelsesområde, i tilfælde hvor anlæggenes funktion er temmelig kvalificerede. Det er dog ikke imod betænkninger og lovforarbejder, da der netop er lagt op til, at bestemmelsen skal have råderum til en analogisk anvendelse[46], og derfor samtidig vil kunne omfatte ikke-objektivt omfattede anlæg, hvis disse vurderes at efterleve de kriterier der er for anvendelsen af bestemmelsen.

Der kan af praksis udledes en tendens ved domstolene i forbindelse med afgrænsningen af bestemmelsens anvendelsesområde for de omfattede anlæg. Der kan f.eks. i dommene U.1981.679

[43] LFF 2003-11-05 nr. 55, pkt. 2.2.1.1
[44] FT, 2003-04, Tillæg A, sp. 1822
[45] LFF 2018-10-03 nr. 20 Ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (freds- og ærekrænkelser m.v.)
[46] Betænkning Nr. 1417/2002 s. 139

B og U.1986.423/2 Ø., ses en klar tendens ved domstolene når det kommer til anvendelsesområdet for Straffelovens § 193, stk. 1. Begge sager omhandler omfattende forstyrrelse i almindelige samfærdselsmidler, hvor det i U.1981.679 B., omhandlede blokadeaktioner ved hjælp af fiskekuttere i forskellige havne. Blokadeaktionen fandt sted både d. 05. maj 1978 mellem kl. 08:00 og kl. 12:00, og igen d. 10. maj 1978 mellem kl. 08:00 og kl. 16:00[47]. Handlingen blev anset som værende en overtrædelse af Straffelovens § 193, stk. 1, da blokaderne i henseende til antal, formål, udstrækning i tid og effektivitet måtte være at anse som værende omfattende, også uanset om et større eller mindre antal færgeankomster eller afgange i de enkelte havne blev forhindret. Det er i denne dom bemærkelsesværdigt, at domstolen udelukkende vægter færgetrafikken højt i vurderingen, og ikke lægger anden havtrafik til grund, i relation til bestemmelsens anvendelsesområde. Dette er dog helt i overensstemmelse med hvad der er objektivt omfattet af almindelige samfærdselsmidler og som tiltænkt i forarbejderne til bestemmelsen.

I U.1986.423/2 Ø., havde 61 lastbilchauffører henstillet deres lastbiler i et vejkryds i København. Dette resulterede i, at trafikken blev blokeret og gennemkørsel i krydset ikke var muligt under blokaden. De tiltalte blev bl.a. tiltalt for overtrædelse af Straffelovens § 193, med begrundelse i, at brugen af private biler, efter samfundsudviklingen, var blevet et "uundværligt led i samfærdslen". Der blev i den forbindelse lagt op til, at udtrykket "almindelige samfærdselsmidler" skulle have et bredere anvendelsesområde, og dermed ikke kun omfatte f.eks. jernbaner, sporveje, dampskibe og luftfartøjer. Der blev i Byretten lagt vægt på af to dommere, at det på baggrund af den stødt stigende forekomst af privatbilisme, at befolkningen i praksis er afhængige af denne transportform. Ydermere ville det efter en umiddelbar sproglig forståelse af "almindelige samfærdselsmidler", samt en formålsfortolkning[48], af bestemmelsen formål være, at sikre transportmidler som offentligheden må kunne påregne at anvende, og derfor også må omfatte privatbilisme[49].

Én dissenterende dommer i Byretten fandt ikke at bestemmelsens formål har haft hensigt til at sikre privatbilismen, men derimod kun offentlige eller private transportmidler som offentligheden har adgang til.[50] De tiltalte blev dog dømt for overtrædelse af Straffelovens § 193.

[47] U.1981.679 B
[48] Strl.bet. af 1923, s. 296
[49] U.1986.423/2 Ø
[50] U.1986.423/2 Ø

Den dissenterende dommers synspunkter fra Byretten blev stort set gengivet i Østre Landsrets afgørelse, hvor det af Landsretten blev lagt til grund, at uanset om privatbilisme efter samfundsudviklingen er at anse som værende en uundværlig del af samfærdslen, fandtes det ikke, at bestemmelsens ordlyd i forening med dennes forarbejder, vil kunne anse privatbilisme omfattet af "almindelige samfærdselsmidler". De tiltalte blev på den baggrund frifundet for overtrædelse af Straffelovens § 193.

Selvom ovenstående domme ikke relaterer sig til datasystemer, kan der på baggrund heraf udledes en tendens hvor domstolene er særdeles varsomme med at foretage udvidende fortolkninger af bestemmelsens anvendelsesområde. Det er for så vidt gældende ved U.1981.679 B, at det ganske i overensstemmelse med lovforarbejderne, er de almindelige samfærdselsmidler – i dette tilfælde offentlig færgetransport, der er objektivt omfattet af bestemmelsen, og det derfor vil være forstyrrelsen i driften af denne type samfærdselsmidler, der må indgå i vurderingen af om gerningsmomentet er opfyldt.
Det er for så vidt gældende for U.1986.423/2 Ø, at selvom det bliver slået fast, at privatbilismen er et "uundværligt led i samfærdslen", at det på trods af dette, ikke vil være objektivt omfattet af bestemmelsen. Dette vil sige, at selv om en analog fortolkning af bestemmelsen reelt er valid at foretage, afstår domstolene fra at foretage en udvidende fortolkning af de objektivt omfattede anlæg i bestemmelsen. Dette er såmænd selvom, at domstolen pointerer, at et "anlæg" såsom privatbilisme eller havtrafik, kan anses som værende "uundværligt", fravælges det, at dette skal opnå beskyttelse under Straffelovens § 193.

Det er på baggrund af ovenstående betænkeligt, at der fra lovgivers side er søgt en så bred definition af begrebet "datasystemer", da det netop vil kunne være grobund for afgræsningsvanskeligheder i praksis. Udtrykket "datasystemer" er, som dette er defineret i lovforarbejderne, stort set altomfattende og vil derfor nyde særdeles bred beskyttelse under Straffelovens § 193. Under datasystemers nuværende definition vil da størstedelen af elektronik falde ind under denne definition og dermed opnå strafferetlig beskyttelse. Med denne definition vil næsten hver eneste person i Danmark besidde mindst ét datasystem, om det værende i form af enten en smartphone, computer eller andet elektronisk udstyr. Der er dog anført i Straffelovrådets betænkning nr. 1563/2017

gjort overvejelser om, at der netop med ændringen af informationssystem til datasystem, er et ønske om at fremtidssikre bestemmelsen, til mulige ikke-teknologiske løsninger[51], hvorfor det i lyset heraf, må ses som et ønske om, at bestemmelsen netop skal have et bredt anvendelsesområde. Det vil i den henseende være op til domstolene at foretage en såkaldt indskrænkende fortolkning af anvendelsesområdet for datasystemer, da der netop i forbindelse med de andre objektivt omfattede anlæg foreligger en tendens til ikke at ville foretage udvidende fortolkning for anvendelsesområdet af bestemmelsen.

Der er i forbindelse med ændringen til datasystemer også tilføjet det forstående udtryk "samfundsvigtige", som giver anledning til fortolkning om, at datasystemer skal have en vis status, og på den vis må adskille sig fra et almindeligt datasystem, for at være omfattet af Straffelovens § 193. Det vil således ud fra en sproglig forståelse give indtryk af, at det så vidt muligt er forsøgt at afgrænse kredsen af de omfattede datasystemer. Der er der interessant om denne nyeste formulering reelt har betydning for kvalificeringen af de omfattede datasystemer, og dette dermed vil kunne afgrænse anvendelsesområdet af bestemmelsen for datasystemer.

3.2.3 Samfundsvigtige

Som belyst i afsnit 3.2.2 er der ud fra lovforarbejderne tale om en særdeles stor "pulje" af datasystemer som vil være omfattet af Straffelovens § 193, og der er så at sige ikke gjort store bestræbelser på kvalitativt at afgrænse hvad disse datasystemer måtte omfatte.

Der foreligger ikke fra lovgivers side megen information om hvilke datasystemer som præcist har været tilsigtet at være omfattet af bestemmelsen udover de objektivt omfattede datasystemer i bestemmelsen, men der kan dog i forarbejderne findes eksempler hvori der nævnes *"[…] værdipapircentralen, kildeskattedirektoratet, politiets motorregistrering eller lignende samt den centrale elektroniske databehandling hos banker og sparekasser, realkreditinstitutter etc."*[52]. Herunder da også *"[…] data inden for værdipapircentralen og SKATs centrale systemer, herunder motorregistret,*

[51] Bet. Nr. 1563/2017 s. 58
[52] Betænkning nr. 1417/2002 s. 123

samt inden for den private sektor angreb med den centrale elektroniske databehandling hos de store banker og sparekasser, realkreditinstitutter mv."[53].

Det er så at sige ikke en opfyldende opremsning af hvilke datasystemer og anlæg der anses som værende samfundsvigtige, men det kan på baggrund heraf, ses at det ikke blot er et hvilket som helst datasystem som vil være omfattet af bestemmelsen, men at det f.eks. inden for det private kun vil være *store* banker og sparekasser, realkreditinstitutter m.v. som vil være omfattet. Hvis det er størrelsen af brugerantallet eller personkredsen som er det afgørende moment, om et datasystem er samfundsvigtigt som, det er anført i forarbejder og betænkninger, vil dette også være det som falder til grund ved vurdering af, om et datasystem må anses for at være samfundsvigtigt. Dette er så vidt yderligere afgrænset af Justitsministeriet hvori der lægges til grund at *"Derimod vil en lammelse eller betydelig driftsforstyrrelse af en bankfilials eller skattekontors dataterminal ikke være omfattet af straffelovens § 193, da virkningerne af driftsforstyrrelsen i disse tilfælde ikke antager den almenskadelige karakter som bestemmelsen forudsætter"*[54].

På denne vis vil brugerfladen, af samtlige af de tilsigtet beskyttede datasystemer, have betydning for samfundsvigtigheden af de ikke-objektivt omfattede datasystemer eller anlæg som fremgår af Straffelovens § 193, stk. 1. Bestemmelsen er så at sige åben til fortolkning for domstolene hvad angår de datasystemer som ikke vedrører driften af anlæg såsom, almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg eller anlæg der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme. Strafbarheden for de ikke-objektivet omfattede datasystemer vil derfor bero på at bestemmelsen kan anvendes analogisk, hvilket der yderligere er gjort tanker om i betænkning nr. 1417/2002[55]. Tanken om den analoge anvendelse kan ligeledes spores helt tilbage til Carl Torps betænkning af 1917 hvori det anføres at "*[…] en saadan Opregning altid maa blive noget vilkaarlig, og at der derfor altid vil kunne rejses Tvivl ved hvilke der er Trang til et saadant Værn, og omvendt kun disse, er medtagne, maa erkendes. Men Ulemperne derved er formentlig væsentlig ringere end Faren ved en Afgrænsning, der holdes i altfor ubestemte og omfattende Udtryk".*[56] Det er således helt tidligt gjort tanker om, at der i takt med samfundsudviklingen altid vil kunne opstå tvivl om hvorvidt et anlæg kun må

[53] LFF 2018-10-03 nr. 20 Ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (freds- og ærekrænkelser m.v.), bemærkning til nr. 3
[54] FT 1984/85 B 1922
[55] Bet. Nr. 1417/2002 s. 139
[56] Strl.bet. 1917, s. 168

tælle, hvis det er objektivt beskyttet af bestemmelsen, eller om en analogisk anvendelse af bestemmelsen vil være nødvendig. Carl Torp har da påpeget i sin betænkning, at det ikke er ønskværdigt at der anvendes alt for ubestemte og omfattende udtryk, da dette netop kan give afgrænsningsproblemer.

Udtrykket "samfundsvigtige" er dermed en ny tilføjelse til Straffelovens § 193, stk. 1, men selvom det ikke fremgår af de tidligere formuleringer af bestemmelsen, har kravet om, at systemet skal være samfundsvigtigt, altid været gældende, og at der dermed ikke har været tilsigtet nogen ændring i bestemmelsens gerningsindhold med formuleringen "samfundsvigtige datasystemer"[57]. Konkluderende er det dog blevet, at omfanget af den berørte personkreds tilstrækkeligt begrænser bestemmelsens rækkevidde hvortil der i betænkninger og lovforarbejder henvises til begrebet "omfattende forstyrrelse"[58]. Samfundsvigtigheden af et datasystem vil derfor skulle foretages på baggrund af hvor omfattende en forstyrrelse har været. Dette giver således anledning til at undersøge hvad der menes med dette begreb, samt hvilke momenter indgår i vurderingen af om en forstyrrelse har været omfattende.

3.3 Omfattende forstyrrelse

For at strafmomentet i Straffelovens § 193 er opfyldt forudsætter det, at fremkaldelsen af forstyrrelsen i driften, af datasystemet skal være omfattende.

Det følger af de helt tidlige betænkninger til den borgerlige straffelov af 1930, at straffelovens § 193 (daværende § 177), er placeret i kapitel 21, da borgerne i almindelighed er interesserede i, at de omtalte anlæg og indretninger ikke forstyrres, og at det af den grund må være en betingelse, at forstyrrelsen er omfattende[59]. Dette giver imidlertid anledning til at undersøge hvad der helt præcist må anses som værende en "omfattende forstyrrelse" samt hvilke elementer der må lægge til grund ved vurderingen af hvornår en handling må anses som værende almenskadelig jf. Straffelovens § 193. Er det alene den berørte personkreds som må ligge til grund ved vurderingen? Er det den tidsmæssige udstrækning af forstyrrelsen som har afgørende betydning for at forstyrrelsen anses som værende omfattende forstyrrende? Er det både personkredsen og det tidsmæssige

[57] Betænkning nr. 1563/2017 s. 201
[58] Betænkning nr. 1032/1985 s. 42.
[59] Strl.bet. 1923, s. 295

aspekt i forening som har betydning for vurderingen? Dette vil søges undersøgt og analyseret i nedenstående afsnit.

Som omtalt ovenfor er det af betænkningerne at Straffelovens § 193 har fundet sin plads i kapitel 21 i Straffeloven er, at *"[…] Almenheden, nemlig Publikum i Almindelighed som [er] interesseret i de Paragraferne ommeldte Indretninger uforstyrrede Funktioneren, der angribes ved Handlingerne."*[60]. Der er således allerede ved den første betænkning til den borgerlige Straffelov gjort tanker omkring anvendelsesområdet for Straffelovens § 193 (daværende § 394). Der lægges i betænkningen af 1912 vægt på, at beskyttelsesobjektet netop er almenheden i almindelighed der søges beskyttet ved indføjelsen af bestemmelsen. Det er dermed vigtigt at have for øje, at de objektivt omfattede anlæg i bestemmelsen vil kunne medføre en almenskadelig virkning hvis forstyrrelsen er fuldbyrdet, da det netop er almenhedens interesse i den uforstyrrede drift som vægtes højt. Hertil gentages yderligere i betænkningen af 1923, at *"For at Handlingen skal være strafbar efter denne Paragraf, er det en Betingelse, at Forstyrrelsen er omfattende. Kun derved antager Handlingen en almenskadelig Karakter."*[6162]. Det bliver her igen gentaget, at bestemmelsens beskyttelsesinteresse, altså almenheden, vil være unægtelig sammenhængende med at forstyrrelsen skal være omfattende.
Ved tilføjelsen af "databehandlingsanlæg" i 1985, synes det en fornødenhed at få, at få klarlagt yderligere *hvornår* en omfattende forstyrrelse i driften vil få den almenskadelige karakter som bestemmelsen, betænkninger og lovforarbejderne forudsætter. Der blev i den forbindelse fremstillet et svar til Folketinget af Justitsministeriet bl.a. at *"De anførte udtryk "omfattende forstyrrelse i driften" og "almenskadelig karakter" angiver, at der må anlægges en kvantitativ vurdering af angrebets omfang. Man må formentlig herved lægge afgørende vægt på størrelsen af den personkreds, der berøres af angrebet."*[63]. Dette er sidste gang at spørgsmålet vedrørende sammenspillet mellem den omfattende forstyrrelse og den almenskadelige karakter er blevet behandlet fra lovgivers side.

[60] Strl.bet. 1912, s. 323
[61] Strl.bet. 1923, s. 296
[62] LFB 1985-05-23 nr. 221
[63] FT 1984/85 B. 1922

Som det kan ses af ovenstående, er det gentagende gange præciseret, at der må lægges vægt på størrelsen af personkredsen ved vurderingen af overtrædelsen af bestemmelsens straffemoment. Der er dog ikke forsøgt at definere en nedre grænse for hvornår en omfattende forstyrrelse må antages ikke at være af den fornødne almenskadelige karakter, hvilket der teoretisk set kan tænkes at måtte foreligge, når det afgørende moment i vurderingen vil afhænge på bl.a. en kvantitativ vurdering af forstyrrelsens omfang.
Det vil i den forbindelse ikke være muligt ud fra høringsnotater, ordlydsfortolkning eller betænkninger, at komme nærmere hvad dette må indeholde, hvorfor det er overhængende at undersøge om dette nærmere kan præciseres i retspraksis. Hertil vil en række domme kunne bidrage til fortolkningen af begrebet "omfattende forstyrrelse".

Det ses i praksis, at skønnet mellem den berørte personkreds kan spænde bredt, afhængigt af sagens omstændigheder. I den senest trykte afgørelse, hvori tiltalte blev tiltalt for overtrædelse af blandt andet Straffelovens § 193, blev der placeret en jernstang på banelegemet ved et jernbanespor, hvilket medførte driftstop og forsinkelse af almindelige samfærdselsmidler i en tidsramme fra klokken ca. 11:45 indtil klokken 14:05. Det berørte anlæg omfattede 272 aflysninger af togafgange samt 104 forsinkelser. I samfærdselsmidlet befandt der sig ca. 120 passagerer[64].
Tiltalte blev kendt skyldig i forholdet og stemmer overens med både ordlyden i bestemmelsen hvori den kriminaliserede handling omfatter forstyrrelsen i driften af almindelige samfærdselsmidler hvor offentlig togtransport er omfattet[65] og som derfor objektivt er omfattet af bestemmelsens beskyttede anlæg. Yderligere kan igen nævnes en dom hvori forsinkelse og aflysninger af almindelige samfærdselsmidler måtte indstilles i flere timer hvorefter at ca. 100.000 togpassagerer blev påvirket af hændelsen[66].

Det er på baggrund af ovenstående interessant at undersøge om der måtte foreligge en nedre grænse for henholdsvis den tidsmæssige udstrækning af forstyrrelsen samt den berørte personkreds. I trykt praksis kan henvises til sager hvori den berørte personkreds omfattede et

[64] U.2021.2130 Ø
[65] Betænkning nr. 1917 og 1923
[66] U.2017.160 Ø

landsbysamfund på ca. 80 husstande og 15.000 husdyr hvori vandforsyningen blev afbrudt i flere timer[67] og en anden sag hvori en TV-transmission blev forstyrret i ca. 20 minutter[68] som blev set af et meget stort antal seere.
Det kan udledes af begge domme at der i nugældende praksis foreligger en nedre grænse for forstyrrelsens varighed hvortil denne med et minimum må vare 20 minutter og for så vidt den berørte personkreds må omfatte mindst et samlet antal personer på den samlede mængde af personer som bestående af 80 husstande. Der er så at sige ingen øverste grænse for hvor mange der skal være omfattet af forstyrrelsen hvilket heller ikke er tilsigtet i forarbejderne og betænkningerne til Straffelovens § 193, men der vil dog være en minimumsgrænse, da forstyrrelsens omfang må afgrænses kvantitativt samt skal have en almenskadelig virkning[69]

I forbindelse med fortolkningen af den *kvalitative* afgrænsning bliver der i betænkninger og lovforarbejder henvist til den kvantitative afgrænsning af personkredsen som vurderingselement i henseende til hvor omfattende forstyrrelsen er. Dette fremstår dog problematisk set i lyset af det brede anvendelsesområde for datasystemer, hvor der fra lovgivers side er brugt en relativt altomfattende definition af begrebet, samt at den primære afgrænsning for anvendelsen vil falde tilbage på antallet af personer som er berørt af en driftsforstyrrelse. Med denne ræson vil det teoretisk set hverken være til hinder for, at platforme som Facebook, Twitter, YouTube, online-aviser og lignende vil være omfattet af bestemmelsen, hvis det udelukkende er den berørte personkreds som vurderingen vil falde tilbage på.[70]. Det er så at sige muligt at ikke-objektivt beskyttede anlæg vil være omfattet af bestemmelsen, hvis blot et datasystem anvendes som led i formidlingen eller leveringen i forening med personkredsen.
Ovenstående domme har som illustration vist at relativt korte forstyrrelser i driften – helt ned til 20 minutter – vil kunne anses som værende omfattende at de objektivt omfattede anlæg i forening med den berørte personkreds.

[67] U.2005.1357 V
[68] U.2001.1187.Ø
[69] FT 2003-04 Tillæg A, s. 1792
[70] Bet. 1032/1985 og Bet. 1417/2002 s. 139-140

Der foreligger ikke mange domme hvor der reelt bliver taget stilling til anvendelsesområdet og udstrækningen af samfundsvigtige datasystemer, men der kan dog med rette henvises til to sager hvori angrebet har været på et datasystem. Hertil kan som den første nævnes den såkaldte CSC-sag[71], som givetvis er en af Danmarks største hackersager og en utrykt byretsdom afsagt af Retten i Roskilde den 19. december 1996.

I dommen fra Retten i Roskilde var der rejst tiltale for overtrædelse af Straffelovens § 193. I forhold 2 a blev der rejst tiltale for at have fremkaldt omfattende forstyrrelse i driften af et militært anlæg i USA, der bl.a. indeholdt visse sensitive oplysninger udelukkende til tjenstligt brug, hvor der var tilknyttet ca. 5.000 brugere. Tiltaltes angreb havde medført at anlægget havde en forstyrrelse i driften i 9 dage.[72]

Forhold 2 c vedrørte ligeså en forstyrrelse i driften på 3 anlæg hos en vejrtjeneste i USA, der indeholdt operationelle systemer til daglig brug til udarbejdelse af vejrmeldinger over store dele af verden samt forsknings- og udviklingssystemer til forbedring af operationelle systemer. Tiltaltes dekryptering af passwordfiler gav en betydelig forsinkelse i autoriseret arbejde på anlægget, hvilket videre indebar, at autoriserede brugere blev afskåret fra at benytte det[73].

I dommen blev der lagt vægt på i Forhold 2 a, at brugerantal og driftsstop var som anført, at anlægget ikke indeholdt klassificerede oplysninger, men derimod bl.a. forskellige personfølsomme data. Dertil kunne tabet, som følge af forstyrrelsen, ikke opgøres, men det blev konkluderet at der var tale om et betydeligt økonomisk tab. Den tiltalte, blev på den baggrund, fundet skyldig i overtrædelse af Straffelovens § 193. Forhold 2 a, er ud fra en fortolkning af bestemmelsens anvendelsesområde, ikke overraskende omfattet. Forholdet opfylder hermed kravet om omfattende forstyrrelse i driften, da der både var tale om driftstop i 9 dage, samt at 5.000 brugere blev berørt af det uautoriserede angreb. Derudover slår domstolen fast, at anlægget er objektivt omfattet af bestemmelsen. Dette kan dog forekomme betænkeligt, da der var tale om oplysninger udelukkende til tjenstlig brug, samt at den berørte personkreds var anlæggets brugere med autoriseret adgang til anlægget. Domstolen må på trods af dette have vurderet, at angrebet har antaget en almenskadelig virkning på denne baggrund.

[71] U.2015.3615.Ø
[72] Bet. 2002/1417 s. 140-141
[73] Bet. 2002/1417 s. 140-141

I forbindelse med forhold 2 c blev det lagt til grund, at det ene anlæg var operationelt og de to andre til forskning og udvikling. Forsknings- og udviklingsanlægget ansås af domstolen *ikke* som værende objektivt omfattet af Straffelovens § 193[74], hvilket må siges at være korrekt efter en konkret ordlydsfortolkning, både af den nutidige og forhenværende bestemmelses formulering. Det blev endvidere anført i dommen, at det ikke var bevist, at den tiltalte var klar over, at anlæggene tilhørte den amerikanske vejrtjeneste eller overhovedet anlæggenes karakter og brug. Den tiltalte havde dog vidst, at anlæggene tilhørte den amerikanske regering, at autoriseret adgang var forbudt, og at det ene anlæg havde særlig stor regnekraft. Den tiltalte havde ydermere haft en almindelig forståelse af situationen og var klar over, at det drejede sig om regeringscomputere. Retten i Roskilde fandt at den tiltalte i over 200 tilfælde havde brudt ind i computere og havde på den vis accepteret de faktiske konsekvenser af sine handlinger, og på således handlet med forsæt[75].
Den tiltalte blev for forhold 2 c dømt for overtrædelse af Straffelovens § 193 for så vidt angik det operationelle anlæg, og for forsøg hvad angik forsknings- og udviklingsanlægget.
Som det anføres i forbindelse med forhold 2 c, var tiltalte ikke bevidst om, at anlæggende tilhørte den amerikanske vejrtjeneste eller overhoveder anlæggenes præcise karakter og brug. Den tiltalte havde dog kendskab til, at anlæggene i forhold 2 c tilhørte den amerikanske regering.
Dette giver imidlertid anledning til at en vis undren vedrørende forsætspørgsmålet i forbindelse med anvendelsen af Straffelovens § 193. Som det er analyseret i afsnit 3.1, vil det kræve en vis grad af forsæt, selv hvis den tiltalte skal dømmes for overtrædelse af Straffelovens § 193, stk. 1, jf. § 21, stk. 1. Det fremkommer af dommen, at det operationelle anlæg som blev angrebet under forhold 2 c, var objektivt omfattet af bestemmelsen, da det leverede vejrmeldinger til store dele af verden. Dette anså domstolen som værende objektivt omfattet af bestemmelsen, hvilket kan forekomme forståeligt, da almenheden kan have interesse i anlægget uforstyrrede drift, hvilket er i overensstemmelse med lovforarbejderne[76].
Derimod fandt domstolen at der kun kunne dømmes for forsøg på overtrædelse af Straffelovens § 193 ved forsknings- og udviklingsanlægget[77]. Dette er på trods af, at domstolen ikke fandt

[74] Bet. 2002/1417 s. 140-141
[75] Bet. 2002/1417 s. 141
[76] Strl.bet. 1923, s. 293
[77] Bet. 2002/1417 s. 141

anlæggene objektivt omfattet af bestemmelsens anvendelsesområde, og lagde derfor vægt på bl.a. at der var tale om at anlægget tilhørte den amerikanske regering. Det følger om end også af Carl Torps betænkning af 1917, at de omfattede anlæg altid vil være vilkårlige som omtalt i afsnit 3.2, hvorfor vurderingen af vigtigheden af de omfattede anlæg altid vil skulle ske på baggrund af sagens omstændigheder[78]. Dog fremgår det ikke direkte af forarbejderne eller betænkninger til Straffelovens § 193, at offentlige computere eller systemer formodningsmæssigt er objektivt omfattet af bestemmelsen[79]. Det findes derfor betænkeligt, at tiltalte blev dømt for forsøg på overtrædelse af Straffelovens § 193 hvad angår disse anlæg. Det vil, når der omhandler forsøg af Straffelovens § 193, jf. § 21, stk. 1, være afgørende, om personen har haft forsæt til fuldbyrdelse af omfattende forstyrrelse af systemet, og dette synes ikke at være tilfældet ud fra sagens omstændigheder. Tiltalte havde ikke kendskab til systemets karakter og det kan derfor diskuteres om der i den anledning vil være forsæt til forsøg i den henseende.
Alt andet lige kan det af dommen udledes, at det i den konkrete sag, foreligger en stort skøn for hvornår et system eller anlæg er omfattet af bestemmelsen, når forholdet ikke direkte falder under et af de objektivt, omfattede samfundsvigtige datasystemer, som fremgår af lovforarbejderne. Dette skal forstås i lyset af, at der allerede fra domstolenes side, foreligger en tendens til at fortolke de objektivt omfattede anlæg i henhold til forarbejderne.

Den anden dom som vil blive behandlet, er den såkaldte CSC-sag[80]. T1 blev i sagen fundet skyldig i overtrædelse af straffelovens § 263, stk. 3, jf. stk. 2, jf. til dels § 21 og § 291, stk. 2, ved i forening med T2 at have forsøgt at have skaffet sig adgang til et samfundsvigtigt informationssystem tilhørende CSC Danmark A/S, som indeholdt følsomme oplysninger for henholdsvis private og offentlige virksomheder, herunder rigspolitiet. Yderligere blev der rejst tiltale for overtrædelse af straffelovens § 193, stk. 1 for i en periode fra d. 13. februar 2012 til slutningen af august 2012 at have skaffet sig adgang til CSC Danmarks mainframe, hvorunder der blev downloadet store mængder personfølsomme data. Tiltalte blev imidlertid ikke dømt for overtrædelse af straffelovens § 193, stk. 1 eftersom det under bevisførelsen i sagen blev forklaret af vidnet G, *" […] at der ikke var*

[78] Strl.bet. 1917 s. 167
[79] Yderligere pointeret af Helena Lybæk Gudmundsdottir J 2015.107 ff.
[80] U.2015.3615Ø

nedbrud eller andre betydelige forstyrrelser af driften hos CSC som følge af angrebet."[81]. Det anføres endvidere af vidnet G, at fejlrettelser som følge af angrebet allerede var foretaget d. 6. marts 2013. Det bliver yderligere pointeret af Landsretten, at selvom CSC's mainframe blev kompromitteret, medførte dette ikke forstyrrelser i driften på en måde som er omfattet af ordlyden eller forarbejderne til straffelovens § 193, idet at både CSC og dennes kunder både før, under og efter hackingangrebet havde sædvanlig uforstyrret adgang til systemerne[82]. Landsretten lægger herefter ikke vægt på, eller tager til overvejelse, om personkredsens størrelse, potentielt ville kunne lægge til grund for en overtrædelse af straffelovens § 193. Der er så at sige fortaget en "allerede fordi"-afgrænsning for anvendelsen af bestemmelsen, hvor domstolen tillægger personkredsen sekundær betydning for anvendelsen. Dette kan forekomme mærkværdigt, da det netop er cementeret i lovforarbejder at det vil være den kvantitative omfang af et angreb som må tages til overvejelse, for at en handling vil opnå den almenskadelige virkning, som bestemmelsen sigter[83]. Landsrettens begrundelse er på ingen måde forkert i forhold til en ordlydsfortolkning af bestemmelsen, da det netop er et objektivt kriterie, at der skal være sket en omfattende forstyrrelse i driften af det berørte datasystem. Det måtte således også have været kommet Anklagemyndigheden til overvejelse, om tiltale for overtrædelse af straffelovens § 193, stk. 1 var en realistisk tiltale at foreligge Landsretten på baggrund af Byrettens afgørelse, hvor det kategorisk blev afslået, at bestemmelsen var overtrådt, da hackerangrebet manglede den omfattende forstyrrende virkning som bestemmelsen foreskriver.

Det er i anklageskriftet anført, at Hverken CSC eller virksomhedens kunders adgang til systemerne blev forstyrret under genopretningen af systemerne, men Anklagemyndigheden tillægger det bl.a. betydning, at tiltalte skaffede sig adgang til "et samfundsvigtigt informationssystem", herunder til CPR-registret[84]. Det behandles ikke yderligere af domstolen, om angrebet på CSC vil være et angreb på et "samfundsvigtigt informationssystem", men tiltalte blev imidlertid bl.a. dømt for overtrædelse af Straffelovens § 263, stk. 3, jf. stk. 2, hvor skærpende omstændigheder vil gøre sig gældende for forholdet. Det kan i den forbindelse tænkes, at hvis den omfattende forstyrrelse havde været en realitet i sagen, at domstolen havde henført angrebet under Straffelovens § 193, og

[81] U.2015.3615 Ø
[82] U.2015.3615 Ø
[83] FT 1984/85 Tillæg B s. 1922 & FT 2003-04 Tillæg A, s. 1792
[84] U.2015.3615 Ø

dermed vurderet, at angrebet på CSCs informationssystemer var et samfundsvigtigt informationssystem i Straffelovens § 193's forstand.

Der kan af det analyserede domme ses en klar tendens til at der lægges afgørende betydning på den kvantitative udmåling af den berørte personkreds – altså at forstyrrelsen skal være omfattende. Dette stemmer ganske overens med hvad der er tiltænkt for bestemmelsens anvendelsesområde fra betænkninger og lovforarbejder. Der ses dog yderligere en tendens at tillægge vægt på tidsaspektet for forstyrrelsen. Det er om end ikke nævnt i forarbejder eller betænkninger, at dette skal tillægges betydning, men det må hertil granske en sproglig fortolkning af begrebet "forstyrrelse". En forstyrrelse må i sin natur ligeledes have en kvantificerbar udstrækning for at kunne kvalificeres som værende omfattende forstyrrende. Derudover er den tidligst trykte praksis der foreligger vedrørende Straffelovens § 193 i Ugeskrift for Retsvæsen, er sagen omhandlende havneblokaden[85]. I dommen lægger domstolen afgørende vægt på *" […] antal, formål, udstrækning i tid og effektivitet […]"*[86] i relation til vurderingen af om forstyrrelsen var omfattende. Det giver i den anledning god mening for domstolene at tillægge dette betydning i vurderingen af om bestemmelsens gerningsmoment er opfyldt.

3.4 Delkonklusion

Som det kan ses af det ovenstående, er der en stor skønsmæssig vurdering forbundet med anvendelsen af Straffelovens § 193. Der har i forbindelse med lovforarbejder og betænkninger ikke været stort fokus på at få kvalificeret de omfattede datasystemer eller få nærmere afgrænset hvornår en forstyrrelse må anses som værende omfattende. Yderligere vil det for domstolene afhænge af en konkret vurdering, om anlæg, der ikke er objektivt afgrænsede i form af bestemmelsen ordlyd, om disse vil være beskyttet af bestemmelsen. Det er set i praksis, at domstolene er betænkelige ved at udvide anvendelsesområdet for bestemmelsen, hvis ikke anlægget objektivt direkte fremgår af bestemmelsen. Dette er f.eks. set i dommen vedrørende havneblokaden, samt vejspærringen i form af lastbiler. I disse situationer bliver der fra domstolenes side lagt vægt på den tilsigtede anvendelse i relation til forarbejderne, og der afvises dermed eksplicit at udvide

[85] U.1981.679 B
[86] U.1981.679 B

anvendelsesområdet for bestemmelsen, selvom slås fast vedrørende privatbilismen, at denne efter den nuværende samfundsorden må anses som samfundsvigtig.
Omvendt forholder det sig når det vedrører datasystemer[87], hvor det ud fra den fremfundne retspraksis ses en tendens til at lade systemer omfatte af bestemmelsen, på trods af at disse ikke er særskilt oplistet i forarbejder eller betænkninger som beskyttede anlæg. Dette er dog ikke i strid med hensigten af anvendelsesområdet, da det netop fra lovgivers side er brugt en særdeles bred definition af datasystemer. Der ses således en tendens til at lade de fysiske anlæg (f.eks. vandforsyning eller samfærdselsmidler), være underlagt en være særdeles tro fortolkning til forarbejder og betænkninger hvor der ikke er meget plads til udvidende fortolkning, hvorimod datasystemer grundet sin definition vil finde anvendelse i mange tilfælde.
Fælles for vurderingen af anvendelsen er immervæk, at forstyrrelsen skal være omfattende for at opnå den almenskadelige karakter. Der vil således i enhver henseende skulle tages stilling til, at selvom der er sket en forstyrrelse, vil dette ikke automatisk virke som selvstændig opfyldelse af bestemmelsens kriterier. Det er immervæk størrelsen af den berørte personkreds som vil afgøre den almenskadelige virkning.

4. Straffelovens § 193 sammenholdt med udvalgte regler

Straffelovens § 193 gør den omfattende forstyrrelse i driften af bl.a. samfundsvigtige datasystemer strafbar. Straffelovens § 193, stk. 1, har samme strafferamme som Straffelovens §§ 291, stk. 2. Straffelovens § 291 fungerer som værn mod ødelæggelsen, beskadigelsen eller bortskaffelsen af ting, hvorimod Straffelovens § 263, stk. 3 vedrører det at skaffe sig uberettiget adgang til en andens datasystem eller data, hvormed straffen kan stige til 6 års fængsel under særligt skærpende omstændigheder.

Det vil derfor være interessant at undersøge, om der må være visse ligheder mellem disse bestemmelser i relation til Straffelovens § 193.

[87] Hermed også databehandlingsanlæg og informationssystemer

Der er såvel også andre bestemmelser i straffeloven der også beskytter mod indgreb i datasystemer, og som derfor i en vis udstrækning har kontaktflade med straffelovens § 193.

4.1 Straffelovens § 291 om hærværk

Straffelovens § 291 foreskriver, at:

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

Stk. 2. Øves der hærværk i betydeligt omfang, eller af mere systematisk eller organiseret karakter, eller er gerningsmanden tidligere fundet skyld efter nærværende paragraf eller efter § 180, § 181, § 183, stk. 2 og 2, § 184, stk. 1, § 193 eller § 193, kan straffen stige til fængsel i 6 år."

Det er for bestemmelsen ødelæggelsen, beskadigelsen eller bortskaffelsen af tingen som udgør det strafbare element, hvortil beskyttelsesobjektet er "ting, der tilhører en anden". Tingbegrebet i Straffelovens § 291 er forsimplet talt afgrænset til også at omfatte databærende medier med indlagte data, hvorfor sletning eller flytning af data vil være ødelæggelse af en ting.[88] Med den formulering betragtes det databærende medie (computeren, mobiltelefonen, serveren eller harddisken) som forbundet med dets data.[89]

Straffelovrådet har anført at de fleste strafbare forhold som vil være omfattet af Straffelovens § 193 formentlig også vil være omfattet af straffelovens § 291. En overtrædelse af straffelovens § 193 kan dog også tænkes uden at der foreligger hærværk af betydeligt omfang.[90] Det er i den anledning også vigtigt at pointere, at bestemmelserne har hver deres beskyttelsesinteresse. Straffelovens § 193 søger at beskytte almenheden mod omfattende forstyrrelse i driften af bl.a. samfundsvigtige datasystemer, hvorimod Straffelovens § 291 søger at beskytte "ting" mod ødelæggelse, beskadigelse eller bortskaffelse.

Sammenfaldende er det dog at både for Straffelovens §§ 193, stk. 1, og 291, stk. 2, at strafferammen for begge bestemmelser er 6 år. For Straffelovens § 291, stk. 2, vil dette dog kun gøre sig

[88] U.1987.216 Ø
[89] Trzaskowski m.fl. – Internetretten, 3. udgave, s. 599
[90] Betænkning nr. 1032/1985 s. 41.

gældende når dette er sket i betydeligt omfang, eller af mere systematisk eller organiseret karakter. Tillige vil strafferammen være 6 år hvis der er tale om gentagelsestilfælde eller hvis gerningspersonen tidligere er straffet efter en af de oplistede bestemmelser i stk. 2.

4.2 Straffelovens § 293. stk. 2.

Straffelovens § 293, stk. 2, som foreskriver, at den, der *"uberettiget hindrer en anden i helt eller delvis at råde over ting, straffes med bøde eller fængsel indtil 1 år. Straffen kan stige til fængsel i 2 år, hvor der er tale om overtrædelser af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger særligt skærpende omstændigheder."*.
Bestemmelsen har fået sin nuværende ordlyd ved lov nr. 352 af d. 19.05.2004, hvor netop stk. 2 blev tilføjet til bestemmelsen og har til sigte til at omfatte elektronisk rådighedshindring ved bl.a. DDoS-angreb.[91] Det er således ikke blot fysisk rådighedshindring der er omfattet af bestemmelsen, men også elektroniske rådighedshindringer. Straffelovens § 293, stk. 2 adskiller sig på sin vis fra Straffelovens § 193 ved, at det strafbare element i bestemmelsen vil være den uberettigede hindring, hvor det for straffelovens § 193 er den omfattende forstyrrelse i driften[92] der er det strafbare element. Forskellen i det store hele er, at Straffelovens § 193 ikke differentierer *hvordan* den omfattende forstyrrelse i driften foretages, men blot at denne skal være omfattende i relation til den berørte personkreds, hvor ved § 293, stk. 2, at det vil være selve rådighedshindringen som er strafbar, og dermed fratager nogen sin ret til at råde over en ting.

5. Straffelovens § 193 i lyset af Straffelovens § 1 og EMRK art. 7

Det kan på baggrund af analyse af Straffelovens § 193 ses, at bestemmelsen er underlagt et række subjektive vurderingselementer vedrørende kriterier for straffemomentets fuldbyrdelse. Det er i den anledning relevant at undersøge om bestemmelsen i sin nuværende udformning, er konkret nok i sin udformning, at borgerne kan forudse deres retsstilling. Særligt i lyset af datasystemers brede definition samt det *ikke*-kvalificerede kvantitative krav for den omfattende forstyrrelse, vil

[91] Lovforslag nr. 55 af d. 05.11.2003
[92] FT 1984/85 Tillæg B, s. 1922

det kunne efterlade et indtryk af, at bestemmelsen er vag i sin fremstillede form. I den forbindelse vil Straffelovens § 1 og Den Europæiske Menneskerettighedskonvention (EMRK) art. 7, anvendes til fortolkning.

5.1 Legalitetsprincippet

Legalitetsprincippet skal sikre borgerne, at handlinger eller undladelser heraf, kun vil kunne anses som værende strafbare, når den lovgivende magt, har haft hensigt hertil[93].

5.1.2 Straffelovens § 1

Det strafferetlige legalitetsprincip fremgår af Straffelovens § 1. Det følger af bestemmelsen, at *"Straf kan kun pålægges for er forhold, hvis strafbarhed er hjemlet ved lov, eller ganske må ligestilles med et sådant".* Der skal ved dette forstås, at en handling eller udladelse heraf, kun kan straffes hvis det faktisk begåede forhold være en overtrædelse af en materiel lovbestemmelse, der kan udløse straf, eller ligestilles med et forhold, som loven sanktionerer med straf[94]. Dette er imidlertid ikke en holdbar løsning, ifølge Lars Bo Langsted, da det med forudsætning i bestemmelsen, vil være gældende, at borgerne gør brug af loven i relation til deres handlingsgrundlag[95].
Dette giver dermed også anledning til at overveje, om en bestemmelse vil kunne anfægtes i forlængelse af sin klarhed.
Det er ifølge Trine Baumbach, klare og præcise materielle bestemmelser er bedst ud fra en nutidig opfattelse af et strafferetligt legalitetskrav. Hertil anføres at "klarhed" refererer til en bestemmelses ordlyd. Dette vil sige, at der tilsigtes et ideal om, at straffebestemmelser skal være præcise i deres formulering, således at borgeren skal kunne opnå en sikker viden om hvad der er strafbart ved at læse bestemmelsen[96]. Det anføres endvidere at klarhed hænger uløseligt sammen med princippet om forudsigelighed. Forudsigelighed referer ikke til selve retskilden eller ordlyden af en bestemmelse, men derimod til den endelige fortolkning af retsgrundlaget[97]. Dette vil sige, at hvis der må inddrages andre retskilder til fortolkning og forståelse af en bestemmelse, vil dette stadig

[93] Bo Langsted – Strafferettens almindelige del, 6. reviderede udgave, s. 91.
[94] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 152.
[95] Bo Langsted – Strafferettens almindelige del, 6. reviderede udgave, s. 93.
[96] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 157.
[97] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 159

kunne opfylde kravet om forudsigelighed[98]. Det er således kun et ideal, at en bestemmelse skal være klart formuleret, og der gælder teoretisk set ingen grænser for hvor uklar eller bred en bestemmelse må være, da det ifølge Lars Bo Langsted, vil være vanskeligt at tænke, at en domstol tilsidesætter en gyldigt tilblevet lovregel med støtte i Straffelovens § 1[99].

5.2 EMRK art. 7

EMRK indeholder i art. 7, ligesom Straffelovens § 1, et strafferetligt legalitetsprincip. EMRK art. 7, stk. 1, 1. pkt. har følgende ordlyd:

"Ingen kan kendes skyldig i et strafbart forhold på grund af en handling eller undladelse, der ikke udgjorde en forbrydelse efter national eller international ret på det tidspunkt, da den blev begået."

EMRK art. 7, stk. 1, 1. pkt. vedrører i sin fremtræden forbud mod strafbar med tilbagevirkende kraft, men har på baggrund af domstolenes praksis opstillet kvalitative krav til karakteren af hjemmel, før der kan være grundlag for straf[100]. Der stilles dermed også yderligere krav om, at en strafbar handling skal være tilstrækkeligt klart og præcist defineret i det relevante hjemmelsgrund for at straf kan pålægges[101].
Begrebet "ret" i EMRK art. 7 omfatter både love, administrative forskrifter udstedet med hjemmel i lov, international ret (herunder EU-ret), samt uskreven ret i form af f.eks. retspraksis[102]. Der vil derfor ikke være et direkte krav om, at ordlyden af en bestemmelse, skal være så klar i sin ordlyd, at en borger vil kunne forudsige retsstillingen blot ved simpel gennemlæsning af bestemmelsens ordlyd i sig selv.
Dette er yderligere fastslået i retspraksis fra Den Europæiske Menneskerettighedsdomstol (EMD) hvori der i sagen Kokkinakis v. Grækenland blev fastslået:

[98] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 160
[99] Bo Langsted – Strafferettens almindelige del, 6. reviderede udgave, s. 93.
[100] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 247.
[101] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 247-248
[102] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 234

"The Court points out that Article 7 para. 1 (art. 7-1) of the Convention is not confined to prohibiting the retrospective application of criminal law to an accused's disadvantage. It also embodies, more generally, the principle that only the law can define a crime and prescribe a penalty (nullum crimen, nulla poena sine lege) and the principle that the criminal law must not be extensively construed to an accused's detriment, for instance by analogy; it follows from this that an offence must be clearly defined in law. This condition is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him liable."[103]

Som det fremgår af ovenstående, er det slået fast, at straf for en forbrydelse skal være klart defineret i loven for at kunne danne baggrund for domsfældelse. Derimod vil domstolenes fortolkning af en straffebestemmelse bidrage til forståelsen af hvilke momenter der kan fuldbyrde straffemomentet. Det er endvidere anført i Kokkinakis v. Grækenland, at ordlyden af bestemmelser ikke er absolut præcise og kan indeholde vage termer, for at undgå rigiditet og holde bestemmelsen anvendelig i takt med samfundsudviklingen[104]. Det blev på baggrund af det anførte konkluderet, at EMRK art. 7 ikke var krænket, da klageren ved hjælp af den tilgængelige nationale retspraksis kunne indrette sin adfærd[105]. Denne fortolkning vedrørende forudsigeligheden af en bestemmelse er ligeledes gentaget i Mørck Jensen v. Denmark hvor det anføres at:

"It is a logical consequence of the principle that laws must be of general application that the wording of statutes is not always precise. One of the standard techniques of regulation by rules is to use general categorisations as opposed to exhaustive lists."[106]

Der er i dommen yderligere henvist til Kokkinakis v. Grækenland, hvorom der kan være et behov for, at bestemmelser bibeholder en form for uklarhed, for netop at holde straffebestemmelsen anvendelig. Ydermere er dette gentaget i Cantoni v. Frankrig hvori det af EMD står anført at:

"One of the standard techniques of regulation by rules is to use general categorisations as opposed to exhaustive lists. The need to avoid excessive rigidity and to keep pace with changing

[103] Kokkinakis v. Grækenland, dom af 25.05.1993, pkt. 52.
[104] Kokkinakis v. Grækenland, dom af 25.05.1993, pkt. 40.
[105] Kokkinakis v. Grækenland, dom af 25.05.1993, pkt. 40
[106] Mørck Jensen v. Denmark, dom af 18.10.2022, pkt. 38.

circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. The interpretation and application of such enactments depend on practice"[107]

Det er i den henseende ikke uoverensstemmende at der må inddrages retspraksis til at udlede hvad en given retstilstand vil være. Dette vil også relatere sig når der sker en gradvis udvikling af en straffebestemmelses anvendelsesområde, hvor at forandrede omstændigheder vil kunne være forenelige med bestemmelsen, hvis udviklingen er forenelig med forbrydelsens væsen, og kan forudses af borgeren med rimelighed[108], som ses konkretiseret i Streletz, Kessler og Krenz v. Tyskland[109]

Det vil dermed ikke være et krav, at en bestemmelse er kvalitativt afgrænset i form af oplistninger for at følge samfundsudviklingen, og vil derfor fortsat kunne opfylde forudsigelighedskravet ved brug af generelle kategoriseringer, og afgrænsning af en bestemmelse på baggrund af dette, hvorom disse kan være vage, vil ikke være en krænkelse af EMRK art. 7. Tillige vil der heller ikke være en krænkelse af EMRK art. 7, hvis en straffebestemmelse undergår en udvikling i sit anvendelsesområde, så længe denne er rimeligt forudsigelig og konsekvent med essensen af forbrydelsen.

5.3 Delkonklusion

I lyset af ovenstående afsnit kan det konstateres, at førend en krænkelse af EMRK art. 7 vil være realiseret, vil det kræve, at en national lov skal være uforudsigelig i et sådant omfang, at borgeren ikke med rette kan forudsige sin retstilstand. Hertil vil bl.a. uskreven ret indgå i overvejelsen, om borgeren med rimelighed har haft mulighed for at indse retstilstanden. Nogle straffebestemmelser holdes vage og smidige i sin formulering af hensyn til muligheden for at tilpasse sig samfundsudviklingen.

Sammenfattende kan det siges, at på trods af, at Straffelovens § 193, i sin nuværende fremtræden, kan forekomme relativt vag med hensyn til den kvalitative afgrænsning af dens beskyttelsesobjekter - specielt "samfundsvigtige datasystemer", samt den "omfattende forstyrrelse i driften".

[107] Cantoni v. Frankrig, dom af 15.11.1996, pkt. 31.
[108] Baumbach, Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, s. 249
[109] Streletz, Kessler og Krenz v. Tyskland, dom af 22.03.01, pkt. 50.

Dette vil dog ikke være ensbetydende med, at bestemmelsen er i strid med hverken Straffelovens § 1 eller EMRK art. 7.

Det er ud fra lovforarbejder, betænkninger og retspraksis muligt for borgeren at forudsige retstilstanden, hvorom anvendelsesområdet af Straffelovens § 193 fortsat er vilkårlig da Straffelovens § 193's definition af "datasystemer" spænder bredt. Det er imidlertid klarlagt af lovgiver, at bestemmelsen vil være tilstrækkeligt afgrænset i sin anvendelse, da det er en betingelse at forstyrrelsen skal være omfattende. Der vil dog altid skulle skæves til idealet om, at straffebestemmelser skal være klare i deres formuleringer, men som det fremgår af betænkningen til Straffelovens § 193 er der et ønske om, at holde bestemmelsen fremtidssikret mod evt. ikke-teknologiske løsninger[110]. Der er derfor anledning et behov for at holde bestemmelsen smidig i forhold til den øgede digitalisering, og der må dermed på sin vis gås på kompromis med klarhedsidealet. Omvendt påfaldende er det, at det eksplicit anføres i Carl Torps betænkning af 1917 at ulemperne ved at have for brede og ubestemte udtryk kan være farlig, og at lovgiver netop skal være påpasselig med, at bestemmelsen ikke bliver for vag, da en rigid anvendelse af bestemmelsen vil overstige ulemperne ved afgrænsning der holdes i ubestemte og omfattende udtryk.[111]

6. NIS-direktivet som fortolkningsbidrag af omfattende forstyrrelse af samfundsvigtige datasystemer

Europa-Parlamentets og Rådets Direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter NIS-direktivet) blev vedtaget i 2016 og implementeret i dansk ret i maj 2018 og søgte et højere sikkerhedsniveau for net- og informationssystemer i hele Unionen.

For at fremme effektiviteten af NIS-direktivet skulle der oprettes et såkaldt CSIRT (Computer Incident Response Team), som skulle fungere som ét nationalt centralt kontaktpunkt med ansvar for at koordinere spørgsmål vedrørende sikkerheden i net- og informationssystemer[112].

[110] Betænkning nr. 1563/2017, s. 58
[111] Betænkning af 1917, s. 168
[112] Europa-Parlamentets og Rådets Direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, pkt. 31-33

NIS-direktivet omfatter en række sektorer der er vurderet som værende særligt kritiske til opretholdelsen af samfundet – også kaldet operatører af væsentlige tjenester, som vil blive behandlet i afsnit 6.1. Disse sektorer er som oplistet i NIS-direktivet at være energi-, transport-, bank-, sundheds- og vandforsyningssektoren såvel som visse digitale infrastrukturer.
NIS-direktivet er minimumsharmoniseret hvilket bevirkede at medlemslandene kunne vedtage eller bibeholde bestemmelser, som følger af NIS-direktivets formål. Både NIS-direktivet, og de efterfølgende nationale implementeringslove, er horisontale og skal forstås i den forstand, at de dækker alle sikkerhedsbrud af de omfattede sektorer på net- og informationssystemer[113].
Som beskrevet ovenfor blev der med implementeringen af NIS-direktivet gennemført flere love og bekendtgørelser, da lovgiver valgte at opdele administrationen af reglerne med hensyn til de omfattede sektorer, således at administrationen blev forbeholdt de berørte ministerier. Administrationen af de implementerede love skulle ske i overensstemmelse med det såkaldte sektoransvarsprincip. Sektoransvarsprincippets virkning er således, at de enkelte love er udformet specifikt til hver enkelt sektor som loven berører[114]. Sektoransvarsprincippet giver således den enkelte myndighed ansvaret for det område som denne til dagligt varetager i tilfælde af en sikkerhedshændelse[115]. Implementeringslovene som følge af NIS-direktivet er på den baggrund opdelt i henholdsvis transport-, energi-, finans-, bank-, og sundhedssektoren samt visse digitale tjenester.
Implementeringen af NIS-direktivet i dansk ret en række krav og forpligtelser for de såkaldte "operatører af væsentlige tjenester", som leverer tjenester som anses som værende væsentlige for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter[116]. Dette vil blive behandlet i afsnit 6.1.

Det har ud fra den relativt beskedne retspraksis vedrørende anvendelsen af Straffelovens § 193 på datasystemer været vanskeligt for domstolene at forene det brede anvendelsesområde i forarbejderne vedrørende samfundsvigtige datasystemer, samt det at der er ikke gjort store tiltag fra lovgivers side til at kvalificere de omfattede datasystemer af bestemmelsen, hvilket øjensynligt er gjort ud fra en betragtning om, at fremtidssikre bestemmelsen. Dette har dog givet domstolene et

[113] Søren Sandfeld Jakobsen m.fl.: Informationssikkerhedsret, 2021, s. 14
[114] Søren Sandfeld Jakobsen m.fl.: Informationssikkerhedsret, 2021, s. 107-108
[115] Søren Sandfeld Jakobsen m.fl.: Informationssikkerhedsret, 2021, s. 108
[116] NIS-direktivet art. 5, nr. 2, litra a

særdeles bredt spænd for hvornår et angreb på et datasystem vil være omfattet af bestemmelsen når forstyrrelsen i driften af dette datasystem har været omfattende. Det kan derfor, både for domstolene og borgerne, ud fra klarhedsidealet, være ønskeligt at kvalificere gerningsmomenterne i bestemmelsen, således at det en mere entydig anvendelse vil forekomme. Det vil dog imidlertid være muligt at anvende NIS-direktivet til at komme afgrænsningsområdet for *"samfundsvigtige datasystemer"* samt *"omfattende forstyrrelse"* nærmere i lyset af NIS-direktivet som fortolkningsbidrag.[117]

Først vil det være interessant at undersøge om de i NIS-direktivet definerede net- og informationssystemer er forenelige med Straffelovens § 193, stk. 1 definition af datasystemer. Det fremgår af forarbejderne til Straffelovens § 193 ved ændringen af ordlyden af informationssystemer til datasystemer, at datasystemer omfatter computere, databehandlingsanlæg eller andet elektronisk udstyr, hvis udstyret har funktioner svarende til førnævnte. Der er således, som beskrevet i afsnit 3.2, tale om særdeles brede vendinger og definition.

Når der kigges på NIS-direktivets definition af net- og informationssystemer, er denne opdelt i tre led:

"a) et elektronisk kommunikationsnet som omhandlet i artikel 2, litra a), i direktiv 2002/21/EF
b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller
c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse"[118]*.*

Det kan ud fra første øjekast ses at, ligesom Straffelovens definition, er definitionen i NIS-direktivet i samme grad tilnærmelsesvist omfattende af alle former for netværk og elektronik. Sammenfaldene med Straffelovens definition af datasystemer er specielt art. 1, nr. 1, litra b hvor *"enhver anordning [der] udfører automatisk behandling af digitale data",* hvor der i Straffelovrådets betænkning lægges vægt på, at datasystem i højere grad end informationssystem, peger henimod den automatiserede behandling af data[119]. Yderligere bred bliver definitionen i art. 1, nr. 1, litra c af net- og informationssystemer hvoraf "digitale data, som lagres, behandles, fremfindes eller

[118] NIS-direktivet art. 4 nr. 1, litra a-c
[119] Betænkning nr. 1563/2017 s. 59

overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse"[120].

Der kan således argumenteres for, at NIS-direktivets definition af net- og informationssystemer, i samme grad som Straffelovens definition af datasystemer, spænder særdeles bredt. Dertil er definitionen af systemerne samtidig er relativt forenelige.

Det er på baggrund af ovenstående ikke muligt at anvende NIS-direktivets definition af net- og informationssystemer som direkte fortolkningsbidrag til at kvalificere hvad datasystemer i Straffelovens § 193, stk. 1 måtte omfatte. Det er dog imidlertid heller ikke hvad dette projekt har søgt at få afklaret, men som det allerede er redegjort for i projektets analyse af Straffelovens § 193, er det ikke alene et krav, at der er tale om et angreb på et datasystem før at strafmomentet i bestemmelsen er realiseret. Der er såvel også krav om, at de kumulative betingelser om, at systemet/anlægget skal være omfattet af bestemmelsen, at der skal være sket i forstyrrelse, at denne forstyrrelse skal være omfattende, samt at dette skal være fremkommet retsstridigt.
Det har ikke været muligt at komme begrænsningen af samfundsvigtige datasystemer nærmere end hvad der fremkommer af den analyserede retspraksis, samt forarbejderne til straffelovens § 193 – herunder særligt *"værdipapircentralen og SKATs centrale systemer, herunder motorregisteret, samt inden for den private sektor angreb mod den centrale elektroniske databehandling hos de store banker og sparekasser, realkreditinstitutter mv."*[121], og visse andre offentlige datasystemer, som domstolen har anset som værende omfattet af bestemmelsen.
Dette er dog søgt nærmere begrænset i NIS-direktivet hvori det netop fremgår som krav, at der udpeges operatører af væsentlige tjenester, hvilket vil kunne bidrage til en afgrænsning af hvilke net- og informationssystemer, og dermed og datasystemer, som må anses som værende "samfundsvigtige" ud fra en komparativ analyse.

6.1 Operatører af væsentlige tjenester:

I NIS-direktivet fremgår det af art. 5, nr. 1 at medlemsstaterne skal udpege de sektorer og delsektorer som vurderes at være operatører af væsentlige tjenester. Disse operatører er defineret som

[120] NIS-direktivet art. 4, nr. 1, litra c
[121] LFF nr. 20 af den 03.10.2018 – Bemærkning til nr. 3.

værende en offentlig eller privat enhed af en type som omhandlet i bilag II i NIS-direktivet. Det fremgår endvidere af art. 5, nr. 2, litra a-c at *"de i artikel 4, nr. 4) omhandlede kriterier for identificering af operatører af væsentlige tjenester er følgende:*

a) *en enhed [som] leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktivitet*
b) *Leveringen af denne tjeneste afhænger af net- og informationssystemer, og*
c) *En hændelse[122] ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste."[123]*

Som det er affattet i Forslag til lov om ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (freds- og ærekrænkelser m.v.), er det kun den omfattende forstyrrelse af et samfundsvigtigt datasystem som er omfattet af den strafferetlige beskyttelse. Som eksempler er nævnt bl.a. angreb på værdipapircentralen og SKATs centrale systemer, herunder motorregistreret, samt inden for den private sektor angreb mod den centrale elektroniske databehandling hos de store banker og sparekasser, realkreditinstitutter mv.[124]. Denne liste over samfundsvigtige datasystemer er tilnærmelsesvist identisk med den af Straffelovrådets betænkning om datakriminalitet af 1985.[125]

Der ses derfor, i modsætning til forarbejderne til Straffeloven, at NIS-direktivet har gjort sig større bestræbelser på at kvalificere de enkelte operatører af væsentlige tjenester, som fremgår af NIS-direktivets bilag II. Derimod søger direktivet ikke at omfatte samtlige filialer eller datterselskaber som en del af begrebet "operatører af væsentlige tjenester". Som eksempel gives det, at sektorer eller delsektorer som anses for væsentlige, ikke uforbeholdent vil være beskyttelsesobjekt, selvom de samlet set vil være operatører af væsentlige tjenester. Her vil f.eks. luftfartssektoren kunne levere tjenester der af en medlemsstat betragtes som værende væsentlige i form af forvaltning af start- og landingsbaner, men herunder vil en række tjenester kunne betragtes som ikkevæsentlige hvis vedrører butiksområder som er tilknyttet operatøren[126]. Det er således op til det enkelte medlemsland at formidle *hvilke* sektorer af en operatør af væsentlige tjenester som måtte være

[122] Enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer jf. NIS-direktivets art. 4, nr. 7
[123] NIS-direktivet art. 5 nr. 2, litra a-c
[124] LFF 2018-10-03 nr. 20 Ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (freds- og ærekrænkelser m.v.), bemærkninger til nr. 3.
[125] Bet. 1032/1985
[126] NIS-direktivet pkt. 21

beskyttelsesobjekt ud fra en betragtning af væsentligheden for opretholdelsen af det samfundskritiske net- og informationssystem. Hertil kommer dog yderligere en række krav til disse sektorer som vil blive behandlet i de kommende afsnit.
Vandforsyningsanlæg er f.eks. objektivt omfattet af Straffelovens § 193, men vil *ikke* være en operatør af væsentlige tjenester når det vedrører net- og informationssystemer, da vandforsyningen og drikkevand kan leveres uagtet om der måtte ske forstyrrelse af de net- og informationssystemer som er tilkoblet vandforsyningsanlægget[127]. Vandforsyningsanlæg er dermed objektivt omfattet af Straffelovens § 193, stk. 1, men må antage en omfattende forstyrrelse af driften der ikke relaterer sig til et datasystem. Det vil på denne baggrund anvendes som fortolkningsbidrag til forståelsen af *hvilke* datasystemer som er omfattet af bestemmelsen, og hvad der anses som værende samfundsvigtigt. Det kan så at sige lægges til grund, at hvis et datasystem indgår som led i opretholdelsen og distributionen af en tjeneste, men ikke har en afgørende rolle i forbindelse med driften, vil det ikke anses som værende samfundsvigtigt i forhold til de objektivt omfattede anlæg. Dette er så at sige ikke udelukkende for net- og informationssystemer i sig selv, da disse også særskilt vil være underlagt beskyttelse, selvom denne ikke har særlig tilknytning til et objektivt omfattet anlæg.

I relation til fortolkningsbidraget til Straffelovens § 193, stk. 1, er det ikke mange datasystemer som *ikke* vil være omfattet af bestemmelsens anvendelsesområde, og det har derfor været vigtigt, at undersøge om der kan foretages en afgrænsning af de andre kriterier for Straffelovens § 193, nemlig; ”omfattende forstyrrelse” og ”samfundsvigtige”. Det er i det ovenstående blev kvalificeret hvad der i relations til NIS-direktivet bliver anset som værende operatører af væsentlige tjenester – altså hvad der i en komparativ analyse vil kunne kategoriseres som værende samfundsvigtige datasystemer. Det vil derfor yderligere være overhængende at undersøge, om det i lyset af NIS-direktivet vil kunne kvalificeres hvad en ”omfattende forstyrrelse” må indebære, da det i Straffelovens § 193 ikke er afgrænset en nedre grænse, men derimod blot skal berøre en personkreds af en vis størrelse, samt at forstyrrelsen skal have vis en tidsmæssig udstrækning for at antage den almenskadelige virkning som behandlet i afsnit 3.3.

[127] Høringsnotat vedrørende udkast til bekendtgørelse om krav til sikkerheden i visse vandforsyningers net- og informationssystemer, s. 2

Vandforsyning er objektivt omfattet af Straffelovens § 193, men er *ikke* en operatør af væsentlige tjenester når det vedrører net- og informationssystemer, da vandforsyningen og drikkevand kan leveres uagtet om der måtte ske forstyrrelse af de net- og informationssystemer som er tilkoblet vandforsyningsanlægget[128]. Vandforsyningsanlæg er dermed objektivt omfattet af Straffelovens § 193, stk. 1, men må antage en fysisk omfattende forstyrrelse af driften, for at kunne realisere gerningsmomentet i bestemmelsen. Det vil på denne baggrund anvendes som fortolkningsbidrag til forståelsen af *hvilke* datasystemer som er omfattet af bestemmelsen, og hvad der anses som værende samfundsvigtigt. Det kan så at sige lægges til grund, at hvis et datasystem indgår som led i opretholdelsen og distributionen af en tjeneste, men ikke har en afgørende rolle i forbindelse med driften, vil det ikke anses som værende samfundsvigtigt. Dette er så at sige ikke udelukkende for net- og informationssystemer i sig selv, da disse også særskilt vil være underlagt beskyttelse, selvom denne ikke har særlig tilknytning til et objektivt omfattet anlæg.

6.2 Omfattende forstyrrelse i lyset af NIS-direktivet

Som gennemgået i ovenstående følger det af NIS-direktivets art. 5, stk. 2, litra c, at der som led i identificeringen af operatører af væsentlige tjenester vil en hændelse skulle have væsentlige forstyrrende virkninger. Dette læner sig sprogligt op ad det "omfattende forstyrrelse i driften" som fremgår af Straffelovens § 193, stk. 1.

Dette har imidlertid ikke nogen kvalificeret afgrænsning i Straffelovens § 193, udover at den kvantitative størrelse af den berørte personkreds vil indgå som altovervejende afgrænsning til anvendelsen[129]. Derudover har det i praksis ved domstolene tillige indgået i vurderingen, at forstyrrelsen skal have en tidsmæssig udstrækning.

Der er endvidere ikke en egentlig minimumsgrænse for hvor stor personkredsen skal være, før en forstyrrelse som behandlet i afsnit 3.3, vil være omfattende eller en nedre grænse for den tidsmæssige udstrækning af forstyrrelsen. Dette giver domstolene et vis skønsmæssigt råderum for hvornår en forstyrrelse er af en sådan størrelse, at både det tidsmæssige og kvantitative kriterie er opfyldt. Det har som sådan ikke i praksis været besværligt for domstolene at foretage denne

[128] Høringsnotat vedrørende udkast til bekendtgørelse om krav til sikkerheden i visse vandforsyningers net- og informationssystemer, s. 2

[129] FT 1984/85 B 1922 & FT 2003-04 Tillæg A, spalte 1792

vurdering ved de fysisk afgrænsede anlæg i bestemmelsen, da der er set domsfældelse fra helt ned til ca. 80 husstandes levering af vand i flere timer fra et vandforsyningsanlæg[130].
Dette er dog søgt nærmere afgrænset for de sektorspecifikke net- og informationssystemer i NIS-direktivets art. 6, stk. 1, litra a-f, hvori følgende forhold gør sig gældende:

"a) antal af brugere, der er afhængige af de tjenester, som udbydes af den pågældende enhed

b) afhængighed i andre sektorer som omhandlet i bilag II af den tjeneste, der leveres af den nævnte enhed

c) de konsekvenser, som hændelser kan have med hensyn til omfang varighed på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed

d) den nævnte enheds markedsandel

e) den geografiske udbredelse med hensyn til det område, som kunne berøres af en hændelse

f) enhedens betydning med henblik på at opretholde et tilstrækkeligt tjenesteniveau under hensyntagen til tilgængelige alternative måder til levering af denne tjeneste"[131]

Når der igen kigges på ordlyden i NIS-direktivet, er det svært ikke at drage paralleller mellem både ordlyden i Straffelovens § 193, stk. 1, men også til lovforarbejderne og helt tilbage fra de tidlige betænkninger af 1912 og frem. Det er i disse gentagende gange slået fast, at et af de vigtigste momenter i vurderingen af om en forstyrrelse har haft omfattende forstyrrende virkning, vil være den berørte personkreds. Som gentaget vil størrelsen af den berørte personkreds være unægtelig sammenhængende om forstyrrelsen kan anses som værende almenskadelig, hvilket netop er det Kapitel 21 i Straffeloven omhandler[132]. I NIS-direktivet er det således også et afgørende moment i vurderingen om forstyrrelsens væsentlighed, at blandt andet antallet af brugere har betydning i væsentlighedsvurderingen. Ved de forskellige implementeringslove der kom i kølvandet på NIS-direktivet, er disse direktivkonforme, hvor der netop er taget hensyn til en konkret kvalificering af størrelsen på den berørte personkreds eller datamængde samt varigheden af forstyrrelsen. Ydermere er det tilsigtet, at leveringen af den væsentlige tjeneste afhænger af net- og informationssystemer om det værende inden for det offentlige eller private[133]. I forbindelse med identificeringen af

[130] U.2005.1357 V
[131] NIS-direktivet art. 6, litra a-f
[132] LFB 1985-05-23 nr. 221
[133] NIS-direktivet pkt. 20 og 27

operatører af væsentlige tjenester er det pålagt medlemsstaterne at identificere disse i henhold til hver sektor eller delsektor. Disse sektorer vil blive behandlet i nedenstående afsnit.

6.2.1 Forsyningssektoren

I lyset af at flere og flere forsyningstjenester er blevet afhængige af datasystemer som led i leveringen af deres tjenester, blev der i NIS-direktivet taget forbehold for, at angreb på denne type anlæg kan have væsentlige skadevirkninger. Det gælder dog for forsyningssektoren, at Danmark har implementeret eldirektivet i dansk lov[134], hvorfor der allerede før implementeringen af NIS-direktivet har foreligget lovgivning for forsyningssektoren. Der er således ikke implementeret en lov i forbindelse med NIS-direktivet, men der foreligger dog en bekendtgørelse om it-beredskab for el- og naturgassektoren, der i og for sig opstiller minimumstærskler for kvalificeringen af et forsyningsanlæg der er væsentlige for den nationale forsyning.[135]

I bekendtgørelsen fremgår det, at virksomheder, der ejer eller driver anlæg kan kategoriseres i tre kategorier jf. bekendtgørelsen § 9, stk. 1, nr. 1-3:

”1) Kategori 1: Virksomheder der forsyner energimængder på nationalt niveau, med over 250.000 slutforbrugere, eller som håndterer energimængder over 600 MWh/h elektricitet eller over 100.000 Nm3/time.

2) Kategori 2: Virksomheder, der producerer eller forsyner energimængder på regionalt niveau, der forvalter et forsyningsområde med mellem 30.000 og 250.000 slutforbrugere, eller virksomheder, der håndterer energimængder svarende mellem 100 MWh/h og 600 MWh/h elektricitet inden for en sammenhængende del af elsystemet eller mellem 10.000 Nm3/time og 100.000 Nm3/time.

3) Kategori 3: Øvrige virksomheder, der ikke er omfattet af kategori 1 eller 2”

Ovenstående anlæg er således af væsentlig betydning for den nationale forsyning hvis medmindre det kan godtgøres, at anlægget *ikke* anvender forsyningskritiske it-systemer jf. § 9, stk. 2.

[134] Europa-Parlamentets og Rådets direktiv 2009/72/EF af 13. juli 2009 om fælles regler for det indre marked for elektricitet og om ophævelse af direktiv 2003/53/EF som senere er afløst af direktiv 2019/944

[135] Bekendtgørelse nr. 1647 af 28.12.2021 om it-beredskab for el- og naturgassektorerne

Det kan i lyset af bekendtgørelsen konstateres, at der foreligger visse vuderingsmomenter, der er sammenlignelige med NIS-direktivet, på trods af at disse ikke direkte er udledt heraf.

6.2.2 Transportsektoren

NIS-direktivet er implementeret i transportsektoren via Lov om net- og informationssikkerhed i transportsektoren[136] (herefter for dette afsnit; loven) hvori anvendelsesområdet omfatter operatører af væsentlige transporttjenester om disse er offentlig eller privat. Transportenhederne som er omfattet, givent de er væsentlige, er lufttransport, jernbanetransport, søfart inden for Transport-, Bygnings- og Boligministeriets område og vejtransport jf. lovens § 2, nr. 1. Om en transportenhed er væsentlig, vil være om til transportministeren, men denne vurdering af væsentlighed skal tages op til revidering hvert andet år jf. lovens § 3, stk. 1. Hertil vil der i forbindelse af udpegning af væsentlige transportenheder jf. stk. 1, skulle lægges vægt på at:

"1) enheden leverer en transporttjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,

2) Leveringen af transporttjenesten afhænger af net- og informationssystemer og

3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte transporttjeneste."[137]

I henhold til nr. 1, lægges der vægt på, at operatøren leverer en transporttjeneste der er af kritisk betydning for *mobiliteten* i Danmark, samt om operatøren leverer en unik tjeneste *eller* om tjenesten inden for en relativt kort tidshorisont kan erstattes af andre transporttjenester.[138]

I relation til nr. 2, vil det som det fremgår af ordlyden, skal transporttjenesten være afhængig af net- og informationssystemer for at være relevant i forhold til en udpegning af operatører som følge af loven, hvilket ligeledes er i overensstemmelse med NIS-direktivets formål.

I Nr. 3 skal dette kriterie forstås i overensstemmelse med NIS-direktivets art. 6, stk. 1, hvor at en hændelse vil få en væsentlig forstyrrende virkning for leveringen af den nævnte transporttjeneste[139]. I selve væsentlighedsvurderingen efter § 3, stk. 2, nr. 3 vil følgende elementer skulle indgå:

[136] Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren

[137] Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren § 3, stk. 2, nr. 1-3.

[138] Forslag til lov nr. 135 af 07.02.2018 om sikkerhed i net- og informationssystemer i transportsektoren, bemærkninger til § 3.

[139] Forslag til lov nr. 135 af 07.02.2018 om sikkerhed i net- og informationssystemer i transportsektoren, bemærkninger til § 3.

"1) Antallet af brugere, der er afhængige af transporttjenesten.

2) Andre sektorers afhængighed af transporttjenesten.

3) Omfanget og varigheden af de konsekvenser, som hændelser kan have på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed.

4) Den pågældende enheds markedsandel.

5) Det geografiske område, der kan blive berørt af en hændelse.

6) Om der i kraft af alternative måder til levering af den pågældende transporttjeneste kan opretholdes et tilstrækkeligt tjenesteniveau.

7) Sektorspecifikke forhold."[140]

Det kan således ses, at der ved udpegelsen af operatører af væsentlige tjenester i transportsektoren er direkte harmoniseret med NIS-direktivet art. 6, stk. 1, jf. art. 5, stk. 2. Der er yderligere konkretiseret, at en kritisk tjeneste, der er afhængig af digital infrastruktur – eller i sproglig udstrækning samfundsvigtigt datasystem – kan være Naviair eller Banedanmarks signalprogram. Hvis Naviairs overvågningsudstyr eller kommunikationssystem ikke fungerer, vil der ikke være andre operatører, der har kapacitet til at overtage styringen, hvilket ville få væsentlig forstyrrende virkning for flyvning i dansk luftrum. I forhold til Banedanmarks signalprogram, vil et nedbrud i systemet betyde, at alt togtransport på Banedanmarks strækninger vil indstilles. Eftersom at Banedanmark dækker størstedelen af jernbaneinfrastrukturen, vil dette betyde af togtrafikken i Danmark vil blive væsentlig forstyrret[141].

Som fortolkningsbidrag til forståelse af Straffelovens § 193, fremgår det direkte, at almindelige samfærdselsmidler er objektivt omfattet af bestemmelsen. Dette er i retspraksis, på baggrund af lovforarbejder og betænkninger, begrænset til *ikke* at omfatte privatbilisme. Eftersom, at almindelige samfærdselsmidler er objektivt omfattet af bestemmelsen, vil et datasystem der relaterer sig til driften af et sådan anlæg således også være at anse som et samfundsvigtigt datasystem. Dette er dog med forudsætning om, at så længe det er angrebet på datasystemet der forårsager den omfattende forstyrrelse. Dette vil bero på en konkret vurdering af domstolene, men som det ses af retspraksis, foreligger der en tendens til at fortolke de objektive anlæg indskrænkende i relation

[140] Bekendtgørelse nr. 1042 af 06.08.2018 om sikkerhed i net- og informationssystemer i transportsektoren, § 3, stk. 4.
[141] Forslag til lov nr. 135 af 07.02.2018 om sikkerhed i net- og informationssystemer i transportsektoren, Almindelige bemærkninger

til forarbejderne, hvorimod det brede anvendelsesområde for datasystemer, synes at lade sig spænde bredt. Dermed vil loven[142] samt bekendtgørelsen[143] kunne bidrage som fortolkningsgrundlag i relation til afgrænsning af hvilke samfundsvigtige datasystemer, for transportsektoren, som vil være objektivt omfattet af Straffelovens § 193.
Hertil vil der i samme grad som betænkninger og lovforarbejder har tilsigtet for Straffelovens § 193, i relation til samfundsvigtige datasystemer, kunne anvendes en bred fortolkning af begrebet "datasystemer" hvortil den kvantitative afgrænsning af den omfattende forstyrrelse stadig vil være det afgørende vurderingsmoment. Ydermere fører dette til en nærmere kvalificering af de omfattede datasystemer, således at der kan opnås en mere ensartet forståelse og anvendelse af begrebet.

6.2.3 Sundhedssektoren

Selvom sundhedssektoren eller specifikke anlæg af denne karakter er omfattet af ordlyden af Straffelovens § 193, vil der ikke skulle meget fantasi til at forestille sig, hvor samfundsvigtigt og særdeles almenskadeligt det ville være, hvis datasystemer i denne sektor teoretisk set måtte blive ramt af et angreb og tilgængeligheden eller driften af datasystemer potentielt kunne resultere i, at patienter ikke modtager behandling, mister adgangen til lægejournaler osv.
Det er derfor ikke utænkeligt at et sådan angreb ville falde under anvendelsesområdet for straffelovens § 193, hvis forstyrrelsen var omfattende nok, da det er svært tænkt, at et sådant datasystem ikke måtte være samfundsvigtigt ud fra en betragtning om, at borgerne i almindelighed er interesseret i denne type anlægs uforstyrrede drift, da det netop er almenheden bestemmelsen søger at beskytte.

NIS-direktivet blev implementeret i dansk lov med Lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren[144], og gælder for operatører af væsentlige tjenester inden for sundhedssektoren jf. lovens § 1. Sundhedssektoren skal i denne forbindelse forstås bredt, og omfatter institutioner og funktioner der har til formål at fremme sundhed, forebygge og

[142] Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren
[143] Bekendtgørelse nr. 1042 af 06.08.2018 om sikkerhed i net- og informationssystemer i transportsektoren
[144] Lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

behandle sygdom, lidelse og funktionsbegrænsning[145]. Loven definerer en operatør af en væsentlig tjeneste jf. lovens § 2, nr. 1, jf. § 3, stk. 1, nr. 1-3 hvis:

"1) Enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter inden for sundhedssektoren,

2) Leveringen af denne tjeneste afhænger af net- og informationssystemer og

3) En hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste."

Det er derfor også et krav, at før en enhed kan betragtes som en operatør af en væsentlig tjeneste, at en hændelse vil få væsentlig forstyrrende virkning for leveringen af tjenesten jf. § 3, stk. 1, nr. 3. Hvad der skal forstås som væsentlig forstyrrende virkning i relation til dette er det op til Sundhedsministeren at fastsætte nærmere regler herom. Det fremgår af bekendtgørelsens § 2, stk. 1, nr. 3, litra a-e, at før en hændelse kan anses som værende væsentlig forstyrrende skal der være tale om et angreb der skal indebære konsekvenser for:

"a) Sundhedsberedskabet i Danmark, herunder den nationale operative stabs funktion,

b) det regionale sundhedsberedskab,

c) mere end 500.000 borgere, der er omfattet af tjenesten,

d) mere end 50.000 brugere, herunder patienter og sundhedspersoner, der er afhængige af tjenesten, eller

e) mindst en region."[146]

Hermed gælder dog også, at hvis tjenesten som operatøren leverer kan leveres uden understøttelse af net- og informationssystemer i mere end 72 timer, vil lovens § 2, stk. 1, ikke finde anvendelse jf. lovens § 2, stk. 3. Der er på denne vis foretaget en både kvalitativ og kvantitativ afgrænsning af lovens anvendelsesområde, og det vil dermed kunne tænkes, at domstolene vil kunne tillægge denne betydning, hvis der søges at foretage en analog fortolkning af Straffelovens § 193 med inddragelse af sundhedssektoren som et samfundsvigtigt datasystem.

Et potentielt angreb på datasystemer i sundhedssektoren er ikke blot en teoretisk situation. Fra den virkelige verden kan der i nyere tid nævnes ransomware-angrebet på bl.a. Storbritanniens National Health Service (NHS).

[145] Forslag til lov nr. 143 af 7. februar 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren, bemærkninger til § 1.

[146] Bekendtgørelse nr. 458 af 9. maj 2018 om operatører af væsentlige tjenester

6.2.4 Domænenavnssystemer og visse digitale tjenester

Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester[147] opstiller tre kumulative kriterier hvorefter operatører skal anses som værende væsentlige. Hertil er kravene, at 1) enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) leveringen af tjenesten afhænger af net- og informationssystemer og 3) en sikkerhedshændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten jf. lovens § 3, stk. 1.

Implementeringsloven adskiller sig på sin vis fra de andre implementeringslove som behandlet ovenfor, da anvendelsesområdet ikke vedrører et net- og informationssystem der er tilknyttet et fysisk anlæg i samme forstand som ellers gør sig gældende for de øvrige operatører. Anlæggene udgør nærmere aktører af digital infrastruktur og udbydere af digitale tjenester. Mere specifikt står det oplistet, at der i loven forstås ved net- og informationssystemer; Domænenavnesystemer (DNS), DNS-tjenesteudbydere, Topdomænenavneadministrator, Onlinemarkedsplads, Onlinesøgemaskine og Cloud computing-tjeneste.[148] Herefter vil det, som i de ovenforstående operatører, være et kriterie for anvendelsen af bestemmelsen, at disse er væsentlige. Det vil derfor være oplagt at undersøge *hvilke* operatører der anses som værende væsentlige i implementeringslovens forstand.

Lovens opstiller hermed tre kumulative betingelser for hvornår en operatør må anses som værende væsentlig jf. lovens § 3, stk. 1.

Hertil vil en operatør være omfattet hvis 1) enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) leveringen af tjenesten afhænger af net- og informationssystemer og 3) en sikkerhedshændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten[149]. Ved den nærmere afgrænsning til væsentligheden og de omfattede anlæg vil erhvervsministeren kunne fastsætte nærmere regler herom jf. lovens § 3, stk. 3.

---

[147] Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester.
[148] Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester § 2, nr. 10-15.
[149] Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester § 3, stk. 1. nr. 1-3.

De specifikke forhold og afgrænsning for væsentlige operatører er fastsat i bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domænenavnsområdet[150]. Det følger af bekendtgørelsen, at operatører af væsentlige tjenester, specifikt for topdomæneadministratorer, hvis administratoren og dennes koncernforbundne selskaber har mere end 500.000 andenordens internetdomænenavne registreret under topdomænenavnet og for DNS-tjenesteudbydere, hvis udbyderen og dennes koncernforbundne selskaber har 1) rekursive navneservere som mere end 100.000 brugere anvender, eller, 2) autoritative navneservere, som har mere end 100.000 andenordens internetdomænenavne tilsluttet jf. bekendtgørelsens § 1, stk. 2 og 3. Tillige fremgår det at en operatør skal inddrage følgende punkter i væsentlighedsvurderingen; nemlig a) antallet af brugere, der er berørt af hændelsen, b) hændelsens varighed og c) hvor stort et geografisk område, der er berørt af hændelsen[151]. Det er på baggrund af de opsatte kriterier muligt for de enheder som leverer tjenesten, kvalitativt at afgrænse deres væsentlighed eller samfundsvigtighed, ud fra en betragtning af brugerfladen.

Der kan af loven, lovforslag og bekendtgørelsen drages paralleller til Straffelovens § 193 hvori det af loven, retspraksis og forarbejderne tillægges det særligt betydning, at den omfattede personkreds må tillægges en særlig betydning for overvejelsen om skadevirkningen er omfattende[152].

6.2.5 Internetudvekslingspunkter

Internetudvekslingspunkter er ved implementeringen af NIS-direktivet søgt beskyttet som en operatør af væsentlige tjenester. Internetudvekslingspunkter er omfattet af lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.[153]
Et internetudvekslingspunkt skal i lovens forstand forstås som en netfacilitet, der muliggør sammenkobling af mere end to uafhængige autonome systemer, hovedsagelig med henblik på at lette udvekslingen af internettrafik jf. lovens § 2, stk. 1, nr. 1. Sagt en smule forsimplet er

[150] Bekendtgørelse nr. 453 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domæneområdet.
[151] Forslag til lov nr. 144 af 7. februar 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester, bemærkninger til § 5
[152] FT 2003-04 Tillæg A, spalte 1792
[153] Lov nr. 437 af d. 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

internetudvekslingspunkter særdeles vigtige i forbindelse med udvekslingen af informationer både nationalt, men også internationalt, da udvekslingen af datatrafik netop foregår igennem disse.
For at et internetudvekslingspunkt vil blive anset som en væsentlig operatør, vil det være afgørende, at tjenesten

"a) tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,

b) leveringen af denne tjeneste afhænger af net- og informationssystemer og

c) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste."[154]

Dette er søgt nærmere afgrænset i bekendtgørelsen til loven, hvori det fremgår at vurderingen af, om en operatør af et internetudvekslingspunkt kan ses for en væsentlig operatør jf. § 2, nr. 5, vil der blive lagt vægt på, om operatøren driver et internetudvekslingspunkt, der håndterer en gennemsnitlig daglig datamængde på mere end 200 gigabit pr. sekund.[155]
Hertil vil det i kontekst til loven anses som værende en hændelse af væsentlige konsekvenser hvis hændelsen medfører 1) nedgang i operatøren kapacitet i forhold til at håndtere data på mindst 50 procent i mindst en time, eller 2) tab af autenticitet, integritet eller fortrolighed.[156]

Gældende for både domænenavnssystemer, visse digitale tjenester og internetudvekslingspunkter gælder at disse anlæg ikke vil falde under de mere fysisk begrænsede anlæg og vil derfor relatere sig datasystemer i deres "rene form". Det kan således tænkes at disse typer af datasystemer vil kunne fortolkes som værende

[154] Lov nr. 437 af d. 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. § 2, nr. 5, litra a-c
[155] Bekendtgørelse nr. 454 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter § 1
[156] Bekendtgørelse nr. 454 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter § 8

6.3 Delkonklusion

Det skal i forbindelse med ovenstående analyse af implementeringslovene af NIS-direktivet fastslås, at disse ikke er tilsigtet at skulle anvendes direkte til fortolkning af Straffelovens § 193. Det vil dog i lyset af manglende kvalitativ afgræsning af samfundsvigtige datasystemer kunne tænkes, at domstolene i en grad kan skele til de sektorspecifikke krav for anlæggene når det skal vurderes, om et datasystem for disse sektorer vil være beskyttet af Straffelovens § 193.

NIS-direktivet er næsten implementeret i sin helhed i dansk lov, og implementeringslovene er gennemført direktivkonformt. Udtrykket net- og informationssystem har i samme grad som datasystemer et særdeles bredt anvendelsesområde, men dette er søgt afgrænset i NIS-direktivet ved introduktionen af begreberne ”operatører af væsentlige tjenester” og ”væsentlig forstyrrende virkning”. En operatør af en væsentlig tjeneste vil således også i en sproglig fortolkning læne sig meget op af ”samfundsvigtig”, i den forstand at begge vil vedrøre en enhed eller anlæg der er vigtig for opretholdelsen af bestemte funktioner i samfundet. Det vil således være formålstjenstligt at inddrage disse elementer i vurderingen af anvendelsesområdet for Straffelovens § 193, da der derigennem opnås en mere transparent og forudsigelig retstilstand.

NIS-direktivets art. 6 omhandler den væsentlig forstyrrende virkning, og læner sig igen op ad den ”omfattende forstyrrelse” i Straffelovens § 193, stk. 1. Det er anført i NIS-direktivet, at der ved vurderingen af en væsentlig forstyrrende virkning for operatører af væsentlige tjenester, b.la. vil skulle tillægges en kvantitativ afgrænsning af antallet af berørte brugere. Der er ved de forskellige implementeringslove vedtaget minimumsgrænser i henhold til bl.a. den tidsmæssige udstrækning en forstyrrelse skal antage, datamængden, personkredsen osv. Dette er dog udelukkende afgrænset i Straffelovens § 193, til at omfatte en kvantitativ afgrænsning af den berørte personkreds.

Der er fra lovgiver givet anledning til, at Straffelovens § 193 skal kunne indgå i en analog fortolkning, og det vil i den forbindelse være hensigtsmæssigt, at der opstilles nærmere specifikke grænser, for hvornår et datasystem vil være objektivt omfattet af bestemmelsen, således at denne ikke får så bredt et anvendelsesområde, som bestemmelsen har på nuværende tidspunkt.

7. Konklusion

Projektet søgte at analysere og afklare anvendelsesområdet for Straffelovens § 193, med særligt fokus på omfattende forstyrrelse af samfundsvigtige datasystemer i et nutidigt perspektiv. For at komme dette nærmere blev der analyseret love, retspraksis, lovforarbejder og betænkninger.

Det kan udledes af projektet, at Straffelovens § 193 har været genstand for en række ændringer i sin ordlyd siden dens borgerlige debut i den borgerlige straffelov af 1930. Med tilføjelsen af databehandlingsanlæg i 1985 har denne type anlæg været beskyttet af bestemmelsen, og der har ikke været en nævneværdig udvikling i afgrænsningen af definition siden da.

Det var som mål for projektet at undersøge anvendelsesområdet for samfundsvigtige datasystemer, men det har i lyset af den beskedne retspraksis, juridisk litteratur, samt manglende kvalitative afgrænsning i betænkninger og lovforarbejder ikke været muligt at komme begrebet nærmere end hvad der fremgår af projektets analyse. Definitionen af datasystemer vil i sin nuværende fremstilling være næsten altomfattende, og vil derfor have et særdeles bredt anvendelsesområde. Det har kunne udledes af betænkning nr. 1563/2017, at det ved revisionen af Straffelovens § 193 har været et ønske om at fremtidssikre bestemmelsen i tilfælde af ikke-teknologiske løsninger måtte præsentere sig i fremtiden, og det kan dermed tænkes, at det netop har været med dette for øje, at datasystemer har fået den så brede definition som den har.

Det har dog i lyset af den utrykte dom fra Byretten i Roskilde været muligt at udlede, at offentlige datasystemer er omfattet af bestemmelsens anvendelsesområde, hvorom dette kan diskuteres at være foreneligt med lovforarbejderne. I lyset af CSC-sagen vil datasystemer der indeholder personfølsomme oplysninger tillige tænkes at kunne være omfattet af bestemmelsen. Det kan dog ikke be- eller afkræftes om dette vil være tilfældet, da domstolen afslog, at der var tale om en overtrædelse af Straffelovens § 193, da forstyrrelsen savnede den omfattende forstyrrelse som bestemmelsen forskriver. Straffelovens § 193 blev ikke yderligere behandlet derfra.

Endvidere kan det udledes af projektets analyse, at både lovgiver og domstolene tillægger den omfattende forstyrrelse stor vægt, i forbindelse med anvendelsen af bestemmelsen. Det kan

dermed også konkluderes, at det fra lovgivers side har været hensigten, at det afgørende vurderingsmoment for bestemmelsens anvendelse vil være, at forstyrrelsen i driften har været omfattende førend en realisering af Straffelovens § 193 straffemoment vil være opfyldt. Dertil er det fra lovforarbejderne fastslået, at det er den omfattende forstyrrelse, der vil give forstyrrelsen sin almenskadelige karakter, hvortil der må tillægges en kvantitativ vurdering af angrebets omfang. Det ses dog også i praksis, at dette tillægges afgørende betydning, og har f.eks. været det afgørende moment for afvisning for anvendelsen af bestemmelsen i CSC-sagen. Dertil kan det også konkluderes på baggrund af retspraksis, at domstolene tillægger den tidsmæssige udstrækning af forstyrrelsen betydning. Det har dog ikke været muligt at finde en minimumsgrænse for hvor stor personkredsen eller den tidsmæssige udstrækning af forstyrrelsen vil skulle være, før denne vil anses som værende omfattende.

Det kan yderligere konkluderes, at selvom Straffelovens § 193 fremstår vag og overlader et stort skønsmæssigt råderum for anvendelsesområdet for datasystemer til domstolene, vil denne imidlertid ikke være i strid med hverken legalitetsprincippet i Straffelovens § 1 eller EMRK art. 7.
Det kan på baggrund af analysen af Straffelovens § 1 og EMRK art. 7, konkluderes, at straffebestemmelser i mange tilfælde vil være nødsaget til at have elastiske og vage formuleringer for netop at kunne følge samfundsudviklingen, og datasystemer er med sin placering i Straffelovens § 193, således kvalitativt afgrænset i kriteriet om at systemet skal være omfattende forstyrret i sin drift.

I lyset af implementeringen af NIS-direktivet kan det konkluderes, at Straffelovens § 193 i en sproglig om komparativ fortolkning læner sig meget op ad NIS-direktivets formuleringer af henholdsvis operatører af væsentlige tjenester, væsentlig forstyrrende virkning, samt definition af net- og informationssystemer. NIS-direktivet har ikke kunne bruges som en direkte fortolkning til forståelsen eller afgrænsning af datasystemer eller omfattende forstyrrelse i Straffelovens § 193, stk. 1. Det kan dog tænkes, at domstolene vil kunne foretage en analog fortolkning af bestemmelsen, og dermed kvalitativt afgrænse anvendelsesområdet for bestemmelsen, da der allerede ved tilføjelsen af databehandlingsanlæg i Straffelovens § 193, har været tænkt en mulighed for at denne analoge fortolkning for de ikke-objektivt omfattende anlæg.

Afslutningsvist kan det reflekterende konkluderes, at Straffelovens § 193, stk. 1, står over for en speciel udfordring i og med, at domstolene har udvist en stor fortolkningsloyalitet til lovforarbejderne og betænkningerne, og er derfor stillet over for en udfordring i, at datasystemer har et så bredt anvendelsesområde. Når fortolkningen altid vil falde tilbage på, en vurdering af den kvantitativt berørte personkreds, vil samtlige datasystemer i realiteten være omfattet af bestemmelsen, hvad end disse reelt er samfundsvigtige eller ej, så længe forstyrrelsen har været omfattende.

Litteraturliste

Litteratur:

Knud Waaben & Lars Bo Langsted – Strafferettens almindelige del, 6. reviderede udgave, 2014, Karnov Group Denmark

Lars Bo Langsted – Waaben strafferettens almindelige del, 6. reviderede udgave, 2018, Karnov Group

Trine Baumbach – Det strafferetlige legalitetsprincip – hjemmel og fortolkning, 1. udgave, 2008, Jurist og Økonomforbundets Forlag

Søren Sandfeld Jakobsen (red.), Max Gersvang Sørensen, Mathias Mølsted Andersen, Bent Ole Gram Mortensen & Daniel Hartfield-Traun – Informationssikkerhedsret, 1. udgave, 2021, Ex Tuto Publishing A/S

Jan Trzaskowski (red.), Søren Sandfeld Jakobsen, Susanne Kartoft, Hanne Kirk, Lars Bo Langsted, Thomas Riis, Charlotte Bagger Tranberg & Helena Lybæk Guðmundsdóttir – Internetretten, 3. udgave, 2017, Ex Tuto Publishing

Thomas Elholm, Lasse Lund Madsen, Hanne Rahbæk og Jens Røn – Kommenteret Straffelov Speciel del. 12. omarbejdede udgave, 2022, Jurist- og Økonomforbundets Forlag

Dorthe Høilund – Retssikkerhed og juridisk metode, 2. udgave, 2018, Hans Reitzels Forlag

Carsten Munk-Hansen – Retsvidenskabsteori, 2. udgave, 2018, Djøf Forlag

Domme

U.2021.2130 Ø

U.2017.160 Ø

U.2015.3615 Ø

U.2005.1357 V

U.2002.2007 V

U.2001.1187 Ø

U.1986.423/2 Ø

U.1981.679 B

Utrykte domme

Dom afsagt af Byretten i Roskilde af d.

EU

Europa-Parlamentets og Rådets Direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen

Europa-Parlamentets og Rådets direktiv 2009/72/EF af 13. juli 2009 om fælles regler for det indre marked for elektricitet og om ophævelse af direktiv 2003/53/EF som senere er afløst af direktiv 2019/944

Lovsamlinger

LBKG 2022-09-28 nr. 1360 Straffeloven

Lov nr. 437 af d. 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

Lov nr. 229 af d. 06.06.1985

Lov 352 af den 19. maj. 2004

lov nr. 1719 af d. 27.12.2018

Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren

Lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

Bekendtgørelser:

Bekendtgørelse nr. 454 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

Bekendtgørelse nr. 458 af 9. maj 2018 om operatører af væsentlige tjenester.

Bekendtgørelse nr. 1042 af 6. august 2018 om sikkerhed i net- og informationssystemer i transportsektoren

Bekendtgørelse nr. 1647 af 28.12.2021 om it-beredskab for el- og naturgassektorerne

Bekendtgørelse nr. 453 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domæneområdet.

Bekendtgørelse nr. 458 af 9. maj 2018 om operatører af væsentlige tjenester

Bekendtgørelse nr. 1042 af 06.08.2018 om sikkerhed i net- og informationssystemer i transport-sektoren

Betænkninger

Straffelovrådets betænkning af 1912

Straffelovrådets betænkning af 1917

Straffelovrådets betænkning af 1923

Betænkning nr. 1032/1985

Betænkning nr. 1417/2002

Betænkning nr. 1563/2017

Folketingstidende:

Folketingstidende samling 1984-85, Tillæg A

Folketingstidende samling 1984-85, Tillæg B

Folketingstidende samling 2003-04, Tillæg A

Folketingstidende samling 2018-19, L 20

Lovforarbejder:

Lovforslag til lov nr. 55 af d. 2003-11-05

LFF 2018-10-03 nr. 20 Ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (freds- og ærekrænkelser m.v.)

LFF nr. 20 af den 03.10.2018

Forslag til lov nr. 135 af 07.02.2018 om sikkerhed i net- og informationssystemer i transportsektoren

Forslag til lov nr. 143 af 7. februar 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren

Den Europæiske Menneskerettighedsdomstol:

Kokkinakis v. Grækenland, dom af 25.05.1993

Cantoni v. Frankrig, dom af 15.11.1996

Streletz, Kessler og Krenz v. Tyskland, dom af 22.03.2001

Mørck Jensen v. Denmark, dom af 18.10.2022

Notater

Høringsnotat vedrørende udkast til bekendtgørelse om krav til sikkerheden i visse vandforsyningers net- og informationssystemer

Notat om tilvalg af cybercrime-direktivet

Vejledninger

Vejledning nr. 9872 af 10. maj 2018 Kriterier og krav til operatører af væsentlige tjenester i sundhedssektoren.

Artikler:

Helena Lybæk Guðmundsdóttir – En analyse af straffelovens § 193, Juristen 3.