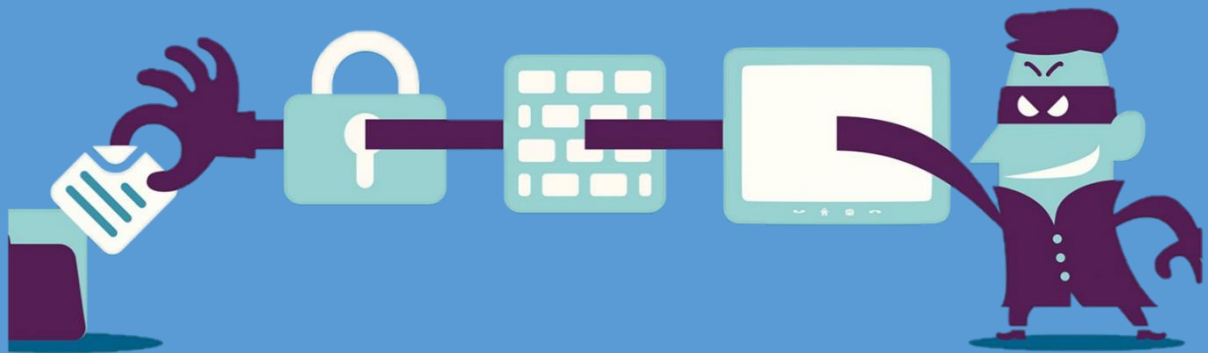


# STRAFFELOVENS § 263, STK. 1

En analyse af straffelovens værn mod hacking

## The Danish Criminal Code section 263(1)

An analysis of the Danish safeguard against hacking



# Titelblad

**Uddannelsesinstitution:** Aalborg Universitet

**Uddannelse:** Jura

**Eksamen:** Kandidatspeciale

**Dansk titel:** Straffelovens § 263, stk. 1 – En analyse af straffelovens værn mod hacking

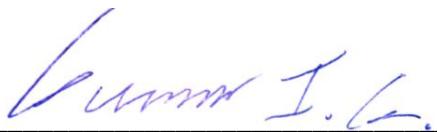
**Engelsk titel:** The Danish Criminal Code section 263(1) – An analysis of the Danish safeguard against hacking

**Afleveret:** 20.05.2019

**Fag:** Strafferet

**Vejleder:** Birgit Feldtmann

**Antal anslag:** 167.573



---

Gunnar Ihlen Gardshodn  
20146384



---

Rasmus Stegenborg Hegelund  
20145760

# Indholdsfortegnelse

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Abstract .....                                                          | 1  |
| Kapitel 1 .....                                                         | 3  |
| 1. Indledning .....                                                     | 3  |
| 2. Formålsformulering .....                                             | 3  |
| 3. Afgrænsning.....                                                     | 4  |
| 4. Metode .....                                                         | 4  |
| Kapitel 2 .....                                                         | 6  |
| 1. Cybercrime .....                                                     | 6  |
| 2. Hacking og den moderne teknologi.....                                | 7  |
| 3. Lovgivningen.....                                                    | 8  |
| 3.1. Dansk lovgivning .....                                             | 8  |
| 3.2. International lovgivning .....                                     | 8  |
| 3.3. EU-retlig lovgivning .....                                         | 9  |
| 4. Baggrunden for det strafferetlige værn .....                         | 10 |
| 4.1. Fredskrænkelser .....                                              | 10 |
| 4.2. Hacking .....                                                      | 11 |
| 5. Negativ afgrænsning af § 263, stk. 1 .....                           | 12 |
| 5.1. § 263a .....                                                       | 12 |
| 6.2. § 264 C .....                                                      | 13 |
| 6.3. § 291 .....                                                        | 13 |
| 6.4. § 293, stk. 2.....                                                 | 14 |
| Kapitel 3 .....                                                         | 15 |
| 1. Introduktion.....                                                    | 15 |
| 2. Data og datasystemer.....                                            | 16 |
| 2.1. En andens data, som er bestemt til at bruges i et datasystem ..... | 16 |
| 2.2. Datasystem .....                                                   | 18 |
| 3. Ubertigtiget .....                                                   | 19 |
| 3.1. Den uberettigede adgang.....                                       | 19 |
| 3.2. Medarbejdere.....                                                  | 22 |
| 3.3. Samtykke eller aftale .....                                        | 25 |
| 3.4. Materiel atypicitet .....                                          | 26 |

|                 |                                                                                 |    |
|-----------------|---------------------------------------------------------------------------------|----|
| 3.5.            | Offentlige eller ikke-offentlige data .....                                     | 27 |
| 3.6.            | Delkonklusion .....                                                             | 29 |
| 4.              | Adgangsbegrebet.....                                                            | 29 |
| 4.1.            | Introduktion.....                                                               | 29 |
| 4.2.            | Hvornår er der opnået adgang? .....                                             | 30 |
| 4.3.            | Kriminalisering af en hypotetisk mulighed? .....                                | 33 |
| 5.              | Betinget offentlig påtale.....                                                  | 34 |
| 6.              | Strafferammen i § 263, stk. 1 .....                                             | 35 |
| 6.1.            | Normalstrafferammen.....                                                        | 35 |
| 6.2.            | Skærpende omstændigheder .....                                                  | 35 |
| 7.              | Grundlæggende strafferetlige principper, menneskerettighederne og hacking ..... | 36 |
| 7.1.            | Straffelovens legalitetsprincip .....                                           | 36 |
| 7.2.            | Den Europæiske Menneskerettighedskonvention .....                               | 38 |
| 7.3.            | Delkonklusion .....                                                             | 40 |
| Kapitel 4       | .....                                                                           | 41 |
| 1.              | Cybercrime direktivet .....                                                     | 41 |
| 1.1.            | Direktivets genstand.....                                                       | 41 |
| 1.2.            | Direktivets definitioner.....                                                   | 41 |
| 1.3.            | De ulovlige handlinger .....                                                    | 43 |
| 2.              | Den svenske lovgivning.....                                                     | 45 |
| 2.1.            | Den svenske hacking bestemmelse .....                                           | 45 |
| 2.2.            | RH 2015:15 – Datasystemer .....                                                 | 46 |
| 2.3.            | NJA 2014 s. 221 – Ulovlig adgang .....                                          | 48 |
| 2.4.            | Sammenfatning .....                                                             | 50 |
| Kapitel 5       | .....                                                                           | 51 |
| 1.              | Retspolitisk vurdering.....                                                     | 51 |
| 2.              | Konklusion .....                                                                | 53 |
| Litteraturliste | .....                                                                           | 55 |

## Abstract

The following project will focus on The Danish Criminal Code section 263 (1), which penalizes the unauthorized access to a data system or data, to be used in a data system. The section itself seems quite simple and straightforward, but the crime can be carried out in many ways, ranging from a simple DDoS, which a 13-year-old can do, to the hacking of servers at major businesses, which requires huge skill and very expensive equipment.

The question then arises, are we sufficiently protected, from a penal view, against cybercrime, or should the current legislation be revised?

The overall method used is the legal dogmatic method. The project aims to analyze and describe the application of the hacking provision. In doing so the project includes the wording of the provision, the preparatory work of the Committee, case law and international sources of law i.e. the Cybercrime convention and the EU Framework decision. After describing the application of the Danish hacking provision, the project then shifts the focus to comparing the Danish application to the similar Swedish hacking provision. Finally, the project includes reflections on the findings in previous chapters.

The project is in 5 chapters, each contributing to the overall understanding of section 263 (1). Chapter 1 is a general introduction to the project, which contains a description of the problem, the method used and the overall structure of the project. Chapter 2 accounts for key IT terms, the relevant legislation (Danish, EU and international law), the reason for having a penal protection against hacking, and a negative delimitation in relation to section 263 (1). Chapter 3 analyzes section 263 (1) by dissecting the individual constituents of the provision and setting the provision up against the principle of legality in The Danish Criminal Code section 1 and the European Human Rights Convention art. 8. Chapter 4 analyzes and compares the provision relevant to hacking in the Cybercrime Directive and The Swedish Criminal Code chapter 4 section 9 C with the Danish criminalization of hacking. Chapter 5 rounds off the project by containing a judicial review of section 263 (1) and an overall conclusion.

The project concludes that the wording of the Danish hacking provision is vague and broad. This paired with the lack of contributions to the interpretation of the provision, the scope of application is left virtually unlimited, which makes it difficult to apply.

In determining if an act is committed *without right* in the provision, the assessment needs to implement a reasonable expectations test. The assessment can take into consideration circumstances such as the relation between the involved parties, consent, the principle of material atypicality etc.

The project also concludes that, the definition of data and data systems includes almost every system imaginable. On the other hand, the Framework decision which has been implemented in Danish law alludes to a limit for minor offences. The delimitation problem arises when certain data and data systems are accessed which lack the need for protection. However, there is not case law nor Committee reports that describe such minor offences.

In terms of *access* there is only a brief statement from the Committee, stating that the requirement has been satisfied, where the perpetrator has gained connection to the contents of the system, and that whether he actually reads or sees the information is irrelevant.

The project concludes that the Swedish hacking provision, as opposed to the Danish, offers more clarity in terms of data/data systems. Swedish case law furthermore considers cases where the access is aimed at standard system files, as minor offences.

In the courts assessment of whether an act is carried out *without right*, the court applies the term in a broad sense. This means that an employee, albeit provided with authorised access, is not necessarily exempted from punishment. In Danish law the main rule is the opposite.

# Kapitel 1

## 1. Indledning

Den 12. marts 2019 kunne the World Wide Web fejre 30-års fødselsdag. I den anledning ytrede Tim Berners sig om dets udvikling<sup>1</sup>. Internettet er i dag en offentlig plads, en butik, en bank, et lægekantor og meget meget mere. Udviklingen har medført, at alt bliver digitaliseret. Alle vores informationer ligger online, lige fra CPR-nummer til bankoplysninger. Udviklingen har på den ene side medført mange gavnlige effekter, bl.a. givet en talestol til marginaliserede grupper og gjort dagligdagens aktiviteter nemmere. Men der er også en mørk side. Hvor banker tidligere blev røvet med pistoler, foregår det i dag med keyboards. Kriminelle rykker i større grad ud på de digitale markeder, hvor udbytte er større og kriminaliteten sværere at spore.

Denne nye tid fordrer regler, der beskytter borgere og virksomheder mod digitale angreb, men giver de nuværende regler en tilstrækkelig beskyttelse?

Der findes mange måder, hvorpå kriminalitet kan begås på digitalt, men dette projekt vil fokusere på hacking, hvor § 263, stk. 1 indtager en særlig stilling. I sin nuværende udformning er bestemmelsen, rent ordlydsmæssigt, egentlig ganske intetsigende, da den kriminaliserer "*uberettiget adgang til en andens datasystem eller data*", men hvad skal forstås ved *uberettiget adgang*, *datasystem* og *data*?

Hvis en person bryder ind i NETS' system, er det uden tvivl ulovligt, men hvad hvis vedkommende har udnyttet en sikkerhedsbrist i systemet, er det så stadig uberettiget? Eller hvis indtrængningen har været med henblik på at teste deres system (såkaldt etisk hacking)? Vil det ulovlige afhænge af, om handlingen er foretaget for at skaffe sig en vinding, eller gælder der noget helt andet?

Der ligger ikke et krav i den danske regel om, at en sikkerhedsforanstaltning skal overkommes, men kan vi stadig snakke om hacking, såfremt der ikke skal brydes en form for sikkerhedsforanstaltning? Og vil dette åbne op for et uforholdsmæssigt bredt anvendelsesområde?

## 2. Formålsformulering

Formålet med denne afhandling er, at analysere § 263, stk. 1 indgående med henblik på en kortlægning af det strafbare område for hacking. I tilknytning hertil, vil vi sammenligne reguleringen i Danmark med Sverige, samt meget kort benævne retstilstanden i de øvrige EU lande.

Afslutningsvis vil vi komme med nogle friere retspolitiske overvejelser over de fremkomne konklusioner.

---

<sup>1</sup> <https://webfoundation.org/2019/03/web-birthday-30/>

### 3. Afgrænsning

Da hacking typisk foregår via internettet giver det anledning til jurisdiktionsspørgsmål. Indragelsen af disse spørgsmål vil imidlertid sprænge rammerne for denne afhandling, og vil derfor ikke blive behandlet.

Hvorvidt hardware-hacking også er omfattet af § 263, stk. 1, er en særdeles interessant problemstilling. Der er imidlertid ingen litteratur eller praksis, der behandler spørgsmålet, hvorfor vi ikke vil behandle hardware-hacking.

Afhandlingen kommer primært at behandle § 263, stk. 1., men da andre bestemmelser i straffeloven i lighed med hackingbestemmelsen berører data, vil disse blive nævnt i det omfang, de bidrager til en afgrænsning af anvendelsesområdet for hackingbestemmelsen, men vil ikke blive analyseret indgående. Øvrig lovgivning vil blive nævnt i det omfang det findes relevant.

§ 193 kriminaliserer det at skabe omfattende forstyrrelse i driften af en række nærmere specificerede systemer. Den kriminaliserede handling kan indebære, at der skaffes adgang til systemet som led i skabelsen af forstyrrelsen, og lægger sig derfor op ad § 263, stk. 1. Særligt i lyset af NIS direktivet<sup>2</sup>, kan der være nogle spændende problemstillinger i forhold til § 193. Af hensyn til specialets omfang, vil vi dog ikke behandle § 193.

Vi ønsker ikke at behandle spørgsmålet, om hvorvidt hackingbestemmelsen udgør en begrænsning af menneskerettighederne, herunder af ytringsfriheden og pressefriheden for journalister.

Da hacking som nævnt angår data, kan det forekomme, at der ved hjælp af hacking, opnås adgang til data der er omfattet af persondataloven. Persondatalovgivningen vil ikke blive behandlet.

Vi behandler i projektet strafferammerne i § 263, stk. 1 og stk. 3. Grundet den sparsomme praksis på området, vil det dog savne mening at analysere bestemmelseernes generelle strafniveau.

### 4. Metode

Specialet er først og fremmest en retsdogmatisk fremstilling, af det strafbare område for straffelovens § 263, stk. 1. Den retsdogmatiske fremstilling er kendetegnet ved at analysere og beskrive gældende ret<sup>3</sup>. De individuelle elementer af straffelovens § 263, stk. 1 vil blive inddelt og analyseret. Denne systematik giver mulighed for at navigere i bestemmelsens gerningselementer og praksis. Det er ikke den retsdogmatiske fremstillings opgave, at løse eventuelle uklarheder i retstilstanden. Hvor der i analysen opstår uklarheder, vil disse derfor blive beskrevet. De retskilder der inddrages i analysen, er fortrinsvis loven, de dertilhørende forarbejder og retspraksis.

Lovens placering som den højst vægtede retskilde, skyldes at denne er vedtaget af myndigheder, der har demokratisk forankrede beføjelser til at forpligte borgere, og at loven skal følges.

---

<sup>2</sup> 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

<sup>3</sup> Munk Hansen – *Retsvidenskabsteori*, s. 204.

For så vidt angår internationale retskilder, har Danmark ratificeret Europarådets konvention om IT-kriminalitet (budapestkonventionen) blev inkorporeret ved lov nr. 352 af 19 maj 2004, hvorfor denne indgår i gældende dansk ret, og vil blive inddraget i analysen. Endvidere er der i EU-regi vedtaget et cybercrime direktiv, hvilket Danmark som følge af retsforbeholdet ikke er forpligtet til at implementere<sup>4</sup>. Dette direktiv, vil derfor ikke indgå i beskrivelsen af gældende ret, men vil dog blive brugt til den komparative del og retspolitiske del.

Retspraksis som retskilde har rødder i en lighedsideologi, hvor det lige skal behandles lige. En tidligere afsagt dom skaber således en retsstilling for andre borgere<sup>5</sup>. Retspraksis vil blive analyseret med henblik på illustration af reglernes anvendelse og fortolkning, samt hvilke hensyn domstolene lægger vægt på. Dommene er udvalgt efter deres evne til at belyse og bidrage til forståelsen af hacking bestemmelsens anvendelsesområde.

Litteratur anses i retsvidenskaben ikke som en retskilde, da litteraturen savner demokratisk legitimitet, og denne ikke skal efterleves af borgere. Litteraturen kan derimod bidrage med andre synspunkter og indfaldsvinkler til forståelsen af de hensyn, der ligger bag bestemmelsen. Litteraturen har derfor også en berettigelse i dette speciale, uden at den dog skal tages til indtægt for gældende ret.

Specialet vil efter den retsdogmatiske del, indeholde et komparativt afsnit hvor der skeles til den tilsvarende svenske Brottsbalken kap. 4, 9c § og cybercrime direktivet. Den anvendte metode er den analytiske metode<sup>6</sup>.

Specialet vil afslutningsvis indeholde nogle retspolitiske bemærkninger. Retspolitikken virke er kendetegnet ved en undersøgelse af mulige løsninger og forslag til et problem ud fra nogle nærmere definerede hensyn<sup>7</sup>. Specialet vil således på baggrund af den forudgående grundige analyse og beskrivelse af gældende ret, præsentere eventuelle problematikker ved bestemmelsen. Disse retspolitiske betragtninger vil tage udgangspunkt i grundlæggende traditionelle juridiske hensyn, som f.eks. hensynet til borgerens retsstilling og kravet om klarhed som forudsætning for idømmelse af straf.

Der er i forbindelse med specialets analyserende arbejde søgt aktindsigt vedrørende anmeldelse i Topdanmark-sagen<sup>8</sup>. Desuden har vi kontaktet Landsretten og Københavns politi for at få en udskrift af pop-up sagen<sup>9</sup>, der analyseres i afsnit 4.2.2. Dog uden held.

Da specialet primært behandler bestemmelser i straffeloven, tilhører nævnte bestemmelser straffeloven, medmindre andet tydeligt anføres.

---

<sup>4</sup> Justitsministeriets notat om tilvalg af cybercrime direktivet, s. 1.

<sup>5</sup> Munk Hansen – *Retsvidenskabsteori*, s. 315-316, samt s. 320.

<sup>6</sup> Munk Hansen – *Retsvidenskabsteori*, s. 72.

<sup>7</sup> Munk Hansen – *Retsvidenskabsteori*, s. 73.

<sup>8</sup> Se herom Topdanmark – Pressemeldelse nr. 20/2010 af 07/12/2010

<sup>9</sup> Østre Landsrets ankedom af 7. marts 2017 – S-2696-16

## Kapitel 2

I dette kapitel gives der i afsnit 1 en generel introduktion til cybercrime. Afsnit 2 fokuserer på hacking og udviklingen heraf set i lyset af den teknologiske udvikling. I afsnit 3 gives der et overblik over retsgrundlaget. Afsnit 4 belyser de hensyn der ligger bag § 263, stk. 1. I afsnit 5 foretages en negativ afgrænsning af § 263, stk. 1. ift. andre strafferetlige bestemmelser, der har en berøring med bestemmelsens anvendelsesområde.

### 1. Cybercrime

Cybercrime er en samlebetegnelse for kriminalitet, der udføres ved hjælp computere og netværk, oftest internettet. De forbrydelser der traditionelt omfattes af dette begreb er hacking, industrispionage, udbredelse af koder til informationssystemer, DDoS (distributed denial of service), elektronisk dokumentfalsk, databedrageri, elektronisk betalingskriminalitet, datahærværk og piratkopiering<sup>10</sup>.

Der findes ingen fast definition af begrebet, men det kan deles begrebet op i to kategorier<sup>11</sup>:

- i. Advanced cybercrime (or high-tech crime) – sophisticated attacks against computer hardware and software;
- ii. Cyber-enabled crime – Traditional crimes that have taken a new turn with the advent of the internet, i.e. crimes against children, financial crimes and terrorism

Lidt forsimplet kan det siges, at forskellen mellem de to kategorier er, at computeren og netværket i den første kategori er *målet* for angrebet, hvor computeren eller netværket i den anden kategori er *midlet* for angrebet.

Hacking kan henføres til begge kategorier. Såfremt hacking i sig selv udgør den kriminelle handling, f.eks. når en person eller gruppe trænger ind i et IT-system, og kræver et beløb for at låse systemet op igen (såkaldt ransomware), vil der være tale om advanced cybercrime. Er hacking derimod blot midlet, f.eks. hvor et it-system hackes for at ødelægge dets data (hærværk, jf. § 291)<sup>12</sup>, vil der være tale om cyber-enabled crime. Cyber-enabled crime er således traditionelle forbrydelser begået ved hjælp af computere, og kan passende beskrives med udtrykket ”gammel vin på nye flasker”.

I sin første betænkning om internetkriminalitet fra 1985 definerede Straffelovrådet ikke cybercrime som sådan, men fastsatte at cybercrime måtte være når der var tale om en strafbar handling, hvorimod det som faldt uden for det strafbare område, måtte karakteriseres som *datamisbrug*<sup>13</sup>.

Cybercrime har udviklet sig meget siden hacking bestemmelsens indførelse, hvor det tidligere blev udført af enkeltpersoner, ser vi i dag store internationale grupper med store færdigheder og dyrt udstyr, der kan ramme store mål.

---

<sup>10</sup> Baumbach – I forskningens og formidlingens tjeneste – *Hacker-bestemmelsen, Se og Hør-sagen og nyere tendenser*, s. 17.

<sup>11</sup> <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> og Lars Bo Langsted m.fl. *Internetretten*, side 586 ff.

<sup>12</sup> Betænkning nr. 1563/2017, s. 51.

<sup>13</sup> Betænkning nr. 1032/1985, s. 14 ff.

Cybercrime har udviklet sig så meget, at WEF i sin rapport *The Global Risks Report 2019* udnævnte visse grene af cybercrime som værende den 4. og 5. største risiko henset til sandsynlighed, og 7. og 8. største trussel henset til skadens potentielle omfang<sup>14</sup>. Dette står i skarp kontrast til det billede som Straffelovrådet tegnede i 1985, hvor cybercrime var af et ringe omfang<sup>15</sup>.

## 2. Hacking og den moderne teknologi

Teknologien har udviklet sig meget siden den første betænkning om cybercrime kom ud i 1985, og det er særligt to områder, der har excelleret og fået cybercrime til at bevæge sig fra angreb begået af enkelte individer, til i dag at blive udført af større kriminelle organisationer.

Den første udvikling er sket i selve tilgængeligheden af teknologien, herunder særdeles operativ systemet. Computere, servere o.lign. opererer jo som sådan på samme måde i dag som for 35 år siden, men udviklingen i operativ systemer, herunder særligt fremført af Microsoft, har gjort computere tilgængelige for alle, uanset ens tekniske niveau.

Den anden udvikling er sket i skabelsen af det moderne internet. I computerens spæde start foregik alle operationer centralt i computeren, men allerede i 1985 blev de første skridt til det moderne internet taget<sup>16</sup>. Internettet fungerer i dag basalt set på samme måde som i 1985, da hele internettet i realiteten består af servere med enormt meget lagerplads, som er koblet op til centrale kabler, hvorigennem langt størstedelen af al data løber<sup>17</sup>.

På et mere teknisk niveau fungerer navigering på internettet ved, at brugeren f.eks. indtaster adressen på en hjemmeside. Herefter sender brugerens egen pc en anmodning til en særlig computer, kendt som en DNS (Domain Name System) server, der omsætter navnet på hjemmesiden til en Internet Protocol (IP-adresse). Brugerens PC sender herefter en anmodning til den pågældende IP-adresse, om at få tilsendt et sæt data. Den pågældende hjemmesides computer bearbejder herefter anmodningen, og tilsender et sæt data, der ved modtagelsen vises på brugerens skærm som tekst, farver og billeder mv.<sup>18</sup>.

Det er særligt udviklingerne inden for selve tilgængeligheden og internettet, der har gjort cybercrime mere populært end nogensinde. Selvom teknologien som sådan stadig bygger på de samme principper, kan der stilles tvivl ved, om vi fortsat har et stærkt nok strafferetligt værn mod cybercrime, da næsten alle informationer lagres på datasystemer i dag. Bør vi derfor gentænke den måde vi kriminaliserer cybercrime på?

---

<sup>14</sup> World Economic Forum – *The Global Risks Report 2019*, s. 5.

<sup>15</sup> Betænkning nr. 1032/1985, s. 16.

<sup>16</sup> Betænkning nr. 1032/1985, s. 12.

<sup>17</sup> Samuel Kerr – *The Problem of Perspective in Internet Law*, s. 360.

<sup>18</sup> Samuel Kerr – *The Problem of Perspective in Internet Law*, s. 363.

### 3. Lovgivningen

Projektets fokus er som nævnt § 263, stk. 1. Som det vil fremgå, er der både på det internationale og EU-retlige plan vedtaget lovgivning, der har en indflydelse på bestemmelsen. Det er derfor hensigtsmæssigt at give et overblik over det nationale, internationale og EU-retlige retsgrundlag.

#### 3.1. Dansk lovgivning

Den nugældende § 263, stk. 1, blev indført ved lov nr. 229 af 06/07/1985 på baggrund af Straffelovrådets betænkning nr. 1032/1985. Bestemmelsen blev da indført som § 263, stk. 2.

Bestemmelsen har siden undergået fire lovændringer. Første revision skete ved lov nr. 6 af 03/01/1992, hvor strafmaksimum i § 263, stk. 3 og § 264, stk. 2 ændredes fra 2 til 4 år<sup>19</sup>. Lovændringen byggede på betænkning nr. 1211/1990. Bestemmelsen blev ændret igen ved lov nr. 433 af 31/05/2000, hvor hæftestrafen udgik<sup>20</sup>. Lovændringen byggede på betænkning nr. 1355/1988. Bestemmelsen blev ændret ved lov nr. 352 af 19/05/2004, hvor den undergik mindre ændringer i ordlyden<sup>21</sup>. Lovændringen byggede på betænkning nr. 1417/2002, der var afgivet af Brydensholt udvalget. Denne lovændring implementerede den EU-retlige rammeafgørelse 2005/222/RIA (omtales nedenfor).

Bestemmelsen er senest revideret ved lov nr. 1719 af den 27/12/2018, hvor den nu indgår som stk. 1 til § 263. Ændringerne i ordlyden og navnlig de overvejelser der ligger i betænkningerne bag lovændringerne er genstand for analyse i kapitel 3.

#### 3.2. International lovgivning

International ret angår det legale forhold mellem suveræne stater<sup>22</sup>. Der kan stilles spørgsmål ved, hvor bindende folkeret faktisk er, da det i sidste ende beror på staternes velvilje til at følge traktaterne, men vi vil behandle dette efter folkerettens ønskelige mål om traktaters binding, som fremsat i Vienna konventionens artikel 26 *Pacta Sunt Servanda*.

Danmark ratificerede den 21/06/2005 Europa Rådets Konvention om cybercrime, også kaldet Budapest Konventionen. Konventionen indebærer, at de kontraherende stater forpligter sig til at foretage justeringer og kriminaliseringer i national ret, der afspejler konventionens artikler.

I forlængelse af konventionen om cybercrime har Europa Rådet udstedt en *Explanatory report*. Rapporten indeholder fortolkningsbidrag til konventionens artikler. De er ikke bindende<sup>23</sup>, men kan dog være behjælpelige for staternes judicielle retsinstanser.

---

<sup>19</sup> Folketingstidende 1991-92, Tillæg A, sp. 1832.

<sup>20</sup> Folketingstidende 1999-00, Tillæg A, sp. 3810.

<sup>21</sup> Folketingstidende 2003-04, Tillæg A, sp. 1762.

<sup>22</sup> Spiermann – *Moderne folkeret*, s. 1.

<sup>23</sup> Jf. Indledningsordene til rapporten.

### 3.3. EU-retlig lovgivning

På det EU-retlige plan, vedtog Rådet den 24. februar 2005, rammeafgørelse 2005/222/RIA om angreb på informationssystemer. Rammeafgørelsen forpligter Danmark. Formålet med rammeafgørelsen, var at skabe en indbyrdes tilnærmelse af medlemsstaternes strafferetlige lovgivning vedrørende angreb på informationssystemer<sup>24</sup>.

Den 12. august 2013 vedtog Rådet og Europa Parlamentet direktiv 2013/40/EU om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (Cybercrime direktivet).

#### 3.3.1. Cybercrime-direktivet

EU's medlemsstater vedtog i 2009 Stockholm-programmet, der redegør for, at Cybercrime de seneste år er vokset i størrelse, og har ændret karakter. Internationale grupper der lever af at begå kriminalitet på nettet, er opstået, og disse frembyder betragtelige vanskeligheder for medlemsstaternes efterforskning. På baggrund heraf anbefaledes det, at medlemsstaternes hurtigt fik ratificeret Cybercrime-konventionen, at unionen bør fremme politikker og lovgivning, der vil sikre en høj sikkerhed på nettet og hurtigere reaktioner ved cyberangreb, og at Kommissionen bør, hvor det fandtes nødvendigt, fremsætte forslag til præcisering af lovgivning om IT-kriminalitet.

På baggrund af Stockholm-programmet og Haagprogrammet af 2004, fremsatte Kommissionen den 30. september 2010 *Forslag til EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV om angreb på informationssystemer og om ophævelse af Rådets rammeafgørelse 2005/222/RIA*. Formålet med forslaget var at erstatte Rådets rammeafgørelse 2005/222/RIA af 24. februar 2005 om angreb på informationssystemer. rammeafgørelsen var frembragt som et ønske om at forbedre samarbejdet mellem de retlige og andre kompetente myndigheder. En af Kommissionen frembragt rapport af den 14. juli 2008 konkluderede, at de fleste medlemsstater havde gjort betydelige fremskridt, og at gennemførelsesgraden var relativt god. Rapporten anførte imidlertid også, at der siden rammeafgørelsen var sket betydelige ændringer i cyber-angrebene form, herunder særligt brugen af botnet<sup>25</sup>. Der var ikke særlig opmærksomhed på disse nye typer angreb i rammeafgørelsen, hvorfor det fandtes mest formålstjenstligt at udtænke nye metoder til bedre at imødegå den nye trussel.

Direktivet er vedtaget under henvisning til Traktatens art. 83, stk. 1, og er dermed omfattet af retsforbeholdet. Danmark deltog ikke i vedtagelsen af direktivet, og har ej heller senere implementeret det. Danmark har derimod implementeret både Rådets rammeafgørelse 2005/222/RIA og Cybercrime-Konventionen ved lov nr. 352 af 19. maj 2004.

---

<sup>24</sup> Rammeafgørelsen 2005/222/RIA, afsnit 1.

<sup>25</sup> Rapport fra Kommissionen til Rådet KOM(2008) 448, s. 10.

## 4. Baggrunden for det strafferetlige værn

### 4.1. Fredskrænkelser

Hackingbestemmelsen er indplaceret som den første bestemmelse i straffelovens kap. 27 med overskriften *Freds- og æreskrænkelser*. Kapitlets centrale beskyttelsesområde er den "uforstyrrede sfære omkring individet og dets livsførelse"<sup>26</sup>. Goos har defineret den private fred som "*den uforstyrrede nydelse af særeksistensen*"<sup>27</sup>. Goos fremhævede, hvilket Lars Bo Langsted har tilsluttet sig, at fredskrænkelser er de tilbageværende delikter, når angreb på legeme, frihed, ejendom mv. er udskilt<sup>28</sup>.

Det er imidlertid svært helt præcist at definere hvad *fred* og *ære* skal forstås som, da begreberne i sig selv er ganske diffuse og udtryk for den gældende kultur i samfundet. Det er imidlertid ikke særligt væsentligt i forhold til lovfortolkning eller den retspolitiske diskussion, at kunne definere begreberne præcist. Bestemmelserne i kap. 27 divergerer i øvrigt noget i deres udførelsesmåde. Visse udføres igennem gerningsmandens optræden overfor andre, f.eks. ved fremsættelse af trusler (§ 266), andre igennem en ubeføjet indblanding i andres privatliv, f.eks. husfredskrænkelse (§ 264, stk. 1, nr. 1) eller hacking (§ 263, stk. 1)<sup>29</sup>.

Traditionelt set har bestemmelserne om fredskrænkelser rødder i hjemmets fire vægge. Mennesker har en privat fysisk sfære, hvor de har ret til at være i fred. De har ret til at holde nogle oplysninger, telefonsamtaler, beskeder mv. for sig selv. Denne beskyttelse er omfattet af menneskerettighedskonventionens artikel 8 om privatlivets beskyttelse<sup>30</sup>. Den fysiske private sfære har siden 1866 være beskyttet mod uønsket indtrængen. I takt med den teknologiske udvikling hvor private oplysninger i stigende grad lagres på digitale enheder, er der også skabt en elektronisk privatsfære. Med indtroduktionen af internettet, er det nu nemmere for udenforstående at overskride denne elektroniske privatsfære<sup>31</sup>. Hacking bestemmelsen er udtryk for en fortsættelse af den beskyttelse, der tidligere var mest relevant i forhold til brevhemmeligheden.

Bestemmelserne i kap. 27 angår primært den individuelle fred, hvorfor de fleste bestemmelser som udgangspunkt kun finder anvendelse på private personer. Imidlertid kan omstændighederne føre til, at også en juridisk person kan være beskyttet<sup>32</sup>. Det er f.eks. ganske svært at sige, at en virksomhed kan føle sig truet, men virksomheder har som private en privat sfære, hvor de har ret til at holde erhvervshemmeligheder for sig selv<sup>33</sup>.

---

<sup>26</sup> Waaben m.fl. – *Strafferettens Specielle del*, s. 232.

<sup>27</sup> Goos – *Den danske Strafferets specielle Del I*, s. 423

<sup>28</sup> Waaben m.fl. – *Strafferettens specielle del*, s. 232.

<sup>29</sup> Waaben m.fl. – *Strafferettens specielle del*, s. 322.

<sup>30</sup> Baumbach – *I forskningens og formidlingens tjeneste – Hacker bestemmelsen, Se og Hør-sagen og nyere tendenser*, s. 25.

<sup>31</sup> Trzaskowski m.fl. – *Internetretten*, s. 588 f.

<sup>32</sup> Waaben m.fl. – *Strafferettens specielle del*, s. 323.

<sup>33</sup> Trzaskowski m.fl. – *Internetretten*, s. 588 f.

## 4.2. Hacking

Hackingbestemmelsen bygger på betænkning nr. 1032/1985. Betænkningen udgør den første juridiske vurdering af det strafferetlige værn mod cybercrime. Baggrunden for udarbejdelsen af betænkningen var, at undersøge hvorvidt straffelovens daværende bestemmelser, navnlig dem om fredskrænkelser, berigelsesforbrydelser, tingsødelæggelse og brugstyveri, i et tilstrækkeligt omfang beskyttede mod retsstridig tilegnelse, ødelæggelse eller brug af dataudstyr, dataprogrammer eller data. Herudover søgtes det redegjort for, hvorvidt straffelovens daværende bestemmelser gav mulighed for at idømme en tilstrækkelig høj straf i tilfælde af særlig grov datakriminalitet<sup>34</sup>.

Betænkning søgte særligt at belyse 8 områder, hvilke Straffelovrådet fandt var de mest relevante i relation til cybercrime<sup>35</sup>

- 1) Ulovligt indblik i andres data
- 2) Videregivelse af data
- 3) Datateknik som middel til berigelsesforbrydelser
- 4) Beskadigelse og ødelæggelse af dataanlæg og data
- 5) Ulovlig brug af dataanlæg
- 6) Forfalskning af bevismidler
- 7) Modtagelse af penge eller oplysninger efter en forudgående dataforbrydelse
- 8) Tilegnelse eller brug af ophavsretligt beskyttede programmer for databehandling

Selve teknologien fungerer overordnet på samme måde i dag som i 1985, men forbrydelsesformen og omfanget har ændret sig meget. Ved § 263, stk. 1's indførelse, var den største trussel i relation til cybercrime databedrageri, hvorimod det i dag er hacking angreb fra organiserede grupper<sup>36</sup>, og efter politiets seneste cybercrime aktion i form af Operation Power Off<sup>37</sup>, er det klart, at fokus i større grad placeres ved deciderede cyber angreb. Center for Cybersikkerhed har vurderet truslen mod danske myndigheder og private virksomheder som meget høj, for så vidt angår cyberspionage og cyberkriminalitet<sup>38</sup>. I 1985 udgjorde cyberkriminalitet en meget lille del af den samlede kriminalitet, dog var Straffelovrådet allerede dengang opmærksom på, at der formentligt var ganske betydelige mørke tal, da internetkriminalitet typisk begås mod en virksomhed, og denne vil ønske at undgå opmærksomheden<sup>39</sup>. Det samme gør sig nok gældende i dag, da virksomheder sjældent ønsker at blive udstillet som havende dårlig digital sikkerhed.

---

<sup>34</sup> Betænkning nr. 1032/1985, s. 5

<sup>35</sup> Betænkning nr. 1032/1985, s. 18

<sup>36</sup> WEF – *Global Risks Report 2019*, s. 7

<sup>37</sup> <https://politi.dk/rigspolitiet/nyhedsliste/politiet-slaar-ned-paa-ddosangreb/2019/01/28>

<sup>38</sup> Center for cybersikkerhed – *Cybertruslen mod Danmark*, s. 1.

<sup>39</sup> Betænkning nr. 1032/1985, s. 15 ff.

## 5. Negativ afgrænsning af § 263, stk. 1

For en helhedsorienteret forståelse af det danske strafferetlige værn mod cybercrime, herunder hacking, er det formålstjenstligt at give et overblik, over de andre bestemmelser i straffeloven, der også beskytter data, og derfor har en kontakthflade med § 263, stk. 1.

### 5.1. § 263a

Baggrunden for indførelsen af § 263a og 301a var, at Brydesholt udvalget i 2002 overvejede om den beskyttelse § 263, stk. 1 medfører var tilstrækkelig. Udvalget vurderede ud fra udviklingen af IT-anvendelsen, om der var behov for en fremskudt regulering, der relaterede sig direkte til passwordbesiddelsen, og som ikke var afhængig af, at der føres fornødent bevis for forsæt til forsøg eller medvirken til senere kriminalitet<sup>40</sup>.

Herefter blev ved lov nr. 352 af 19/05/2004 bestemmelserne § 263a og 301a indført i straffeloven. Udvalget overvejede i forbindelse hermed, om bestemmelserne skulle indføres samlet eller adskilt. Udvalget gik med sidstnævnte. Herefter skulle § 263a regulere adgangsmidler til ikke kommercielle datasystemer og § 301a de kommercielle datasystemer (datasystemer der er forbeholdt betalende brugere)<sup>41</sup>.

§ 263a og § 301a, skal således ses i sammenhæng med § 263, stk. 1, hvor § 263, stk. 1 regulerer selve fredskrænkelsen, mens § 263a og § 301a yder et strafferetligt værn på et tidligere stadie, navnlig i de tilfælde hvor der skabes mulighed for at skaffe sig adgang til kommercielle og ikke kommercielle datasystemer<sup>42</sup>.

Bestemmelserne blev ved lov nr. 1719 af 27/12/2018 revideret, og findes begge i den nugældende § 263a.

De tidligere § 263a og 301a blev sjældent anvendt, men Straffelovrådet vurderede, at bestemmelserne ikke burde fjernes ved revisionen, da det er vigtigt, at der findes en bestemmelse som, fremskynder det strafferetlige værn for § 263, særligt da bestemmelser som §§ 263a og 301a vil få større relevans, i takt med at mere og mere kriminalitet rykker ud i cyberspace.<sup>43</sup>

Sammenskrivningen af bestemmelserne er hensigtsmæssig, da begge bestemmelser har adgangsmidler til datasystemer som beskyttelsesobjekt. Den ny affattede § 263a regulerer herefter anskaffelse, videregivelse, udbredelse og salg af adgangsmidler til både kommercielle og ikke kommercielle datasystemer. Ved ændringen udgik afgrænsningen *ikke offentligt tilgængeligt informationssystem*. Denne ændring kunne foranledige til den antagelse, at bestemmelsens anvendelsesområde herved udvides. Det fremgår dog af forarbejderne, at de kommercielle datasystemer er omfattet af stk. 1, nr. 3, litra c, og de ikke kommercielle datasystemer er omfattet af stk. 1, nr. 1 og 2.

Ændringen er alene båret af forenklings- og moderniseringshensyn. Der er ikke tilsigtet ændringer i den hidtil gældende retstilstand, hvorfor tidligere forarbejder og praksis stadig er relevant<sup>44</sup>.

---

<sup>40</sup> Betænkning 1417/2002, s. 59.

<sup>41</sup> Betænkning 1417/2002, s. 71.

<sup>42</sup> Toftegaard Nielsen m.fl. – *Kommenteret Straffelov Speciel del*, s. 511.

<sup>43</sup> Betænkning nr. 1563.2017, s. 72.

<sup>44</sup> Folketingstidende, Tillæg A, samling 2018-19, L20, s. 49.

## 6.2. § 264 C

§ 264 c blev indsat ved lov nr. 89 af 29/03/1972, men blev med lov nr. 1719 af 27/12/2018 ændret og har i dag følgende ordlyd:

*De i §§ 263, 264, 264 a og 264 b indeholdte straffebestemmelser finder tilsvarende anvendelse på den, der uden at have medvirket til gerningen uberettiget skaffer sig eller udnytter oplysninger, som er fremkommet ved overtrædelsen.*

Ved ændringen blev ordlyden ændret, således at ordet *uberettiget* nu både dækker anskaffelse og udnyttelse<sup>45</sup>. Bestemmelsen kriminaliserer herefter to former for efterfølgende medvirken jf. udtrykkene *skaffer* og *udnytter*. Oplysningerne skal være fremkommet i forbindelse med, at en eller flere af bestemmelserne i § 263, 264, 264 a eller 264 b objektivt er blevet overtrådt. Det er derimod ikke en forudsætning, at nogen kan drages subjektivt til ansvar for overtrædelsen af de nævnte bestemmelser. De i bestemmelsen omtalte *oplysninger* omfatter oplysninger i enhver form<sup>46</sup>.

Ved *skaffer* menes en aktiv handling i at anskaffe sig oplysninger. Ved *udnytter* menes en mere passiv handling, hvor vedkommende er kommet i besiddelse af oplysningerne på en tilfældig og uhåndgribelig måde, men anvender oplysningerne uretmæssigt. Bestemmelsens primære anvendelsesområde skulle være erhvervsspionage og journalisters offentliggørelse af oplysninger<sup>47</sup>.

Bestemmelsen anvendes ikke ofte, hvilket kan undre en smule, da der i dag er store online sorte markeder, hvor oplysninger indhentet igennem hacking sælges. Bestemmelsen har derfor bestemt en berettigelse i dagens samfund, og den manglende anvendelse kan hænge sammen med manglende jurisdiktion, besværlig efterforskning, eller simpelthen en manglende viden om markedernes eksistens og opbygning.

## 6.3. § 291

§ 291 blev indsat i Straffeloven af 1866 og er senest ændret ved lov nr. 82 af 30/01/2019.

Beskyttelsesobjektet er *ting, der tilhører en anden*. I **U 1987.216 Ø** fastslog Landsretten, at *Databærende medier* med indlagte data må anses for *ting*, hvorefter retten statuerede, at sletning eller flytning af data, således at mediet ikke kan benyttes på sædvanlig vis, er *ødelæggelse af ting*.

Den strafbare adfærd består i ødelæggelse, beskadigelse eller bortskaffelse. I relation til hacking vil det ofte være hackerens mål at tage besiddelse af de eksisterende data på datasystemet, eller simpelthen destruere dataene. Dog kan der stilles det spørgsmål, om det stadig vil være strafbart, såfremt dataene kan genskabes, f.eks. igennem en backup. I sådan en situation kan der i hvert fald straffes for forsøg, jf. § 21.

Mest nærliggende er det nok, at § 291 anses for at være fuldbyrdet, uanset at der eksisterer en backup, netop da dataene er blevet ødelagt, beskadiget eller bortskaffet, se herom U.2018.1787H. En lignende situation foreligger ved andre delvise ødelæggelser, f.eks. graffiti, hvor dette er strafbart efter § 291, selvom den beskadigede ting kan genetableres til sin forhenværende stand, se f.eks. hertil U 1988.372 H.

<sup>45</sup> Folketingstidende, Tillæg A, samling 2018-19, L20, s. 55.

<sup>46</sup> Betænkning 1563/2017, s. 26.

<sup>47</sup> Toftegaard Nielsen m.fl. – *Kommenteret Straffelov Speciel del*, s. 522 & Betænkning 1563/2017, s. 26 f.

#### 6.4. § 293, stk. 2

§ 293, stk. 2 kriminaliserer rådighedshindringer. Bestemmelsen blev ændret ved lov nr. 352 af 19/05/2004, som resultat af betænkning 1417/2002, og lyder i dag:

*Stk. 2. 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.*

Den seneste ændring var begrundet i et behov for at tydeliggøre, at bestemmelsen også dækker datasystemer<sup>48</sup>. Forarbejderne nævner særligt de såkaldte Distributed-Denial-of-Service angreb (DDoS), hvilke stadig er meget aktuelle, se f.eks. Operation Power Off I & II, der begge fokuserer på DDoS angreb. Af andre former for angreb kan nævnes Ransomware angreb, hvilke er steget i popularitet de seneste år.

I relation til hacking er DDoS sjældent af relevans, da formålet med DDoS angreb typisk vil være at overbelaste en server, og herefter kræve et beløb for at stoppe angrebet. Der er således typisk ikke et element af hacking involveret, da der ikke sker en indtrængen i selve datasystemet. Derimod er Ransomware angreb meget relevante, da det kræver en indtrængen, og efterfølgende installation af et program i datasystemet for at fuldføre dette. Et succesfuldt Ransomware angreb burde derfor også være omfattet af § 263, stk. 1.

---

<sup>48</sup> Toftegaard Nielsen m.fl. – *Kommenteret Straffelov Speciel del*, s. 676.

## Kapitel 3

I dette kapitel vil § 263, stk. 1 blive beskrevet og analyseret, med henblik på at fastlægge dets anvendelsesområde. Indledningsvis gives der en introduktion til bestemmelsen. Herefter vil der i afsnit 2, blive gjort rede for bestemmelsens beskyttelsesobjekt *datasystemer* og *data*, som er bestemt til at bruges i et *datasystem*. I afsnit 3 gennemgås udtrykket *uberettiget*. Afsnit 4 behandler begrebet *adgang*. Afsnit 5 behandler påtale reglerne. Afsnit 6 behandler strafferammen og de skærpende omstændigheder. Afsnit 7 undersøger om § 263, stk. 1 er i overensstemmelse med menneskerettighedskonventionens art. 7 og straffelovens § 1.

### 1. Introduktion

§ 263 er den første bestemmelse i straffelovens kap. 27. Bestemmelsens stk. 1 indeholder forbuddet mod ulovlig adgang til andres datasystemer eller data. Stk. 2 indeholder forbuddet om brud på brevhemmeligheden, samt mod uberettiget aflytning. Stk. 3. indeholder en strafskærpselsesregel til de tre forbud.

§ 263, stk. 1 omtales oftest som hacking bestemmelsen. Bestemmelsen omfatter dog, som det vil fremgå, andet og mere end egentlig hacking<sup>49</sup>.

Bestemmelsen var tiltænkt til at skulle ulovliggøre indblik i andres data, og blev indført som et stk. 2 til den eksisterende § 263 ved lov nr. 229 af 06/07/1985, hvor den lød således:

*“Med bøde, hæfte eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.”*

Bestemmelsen er senest revideret ved lov nr. 1719 af den 27/12/2018, hvor den blev flyttet til stk. 1 og har i dag følgende ordlyd:

*“Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem.”*

Ændringen har ifølge bestemmelsens forarbejder, ikke skulle medføre en ændring i anvendelsesområdet, derimod er det tale om en modernisering, som er et udslag af den teknologiske udvikling. Hvor kommunikation, meddelelser og data tidligere var nedfældet på papir, bliver disse i dag i udbredt grad lagret på elektroniske medier<sup>50</sup>. På denne baggrund blev det anset for mere naturligt, at lade § 263, stk. 1 udgøre det fremtidige udgangspunkt for beskyttelsen af brevhemmeligheden. Dog stadig med supplerende beskyttelse af de mere traditionelle breve, lukkede meddelelser og optegnelser<sup>51</sup>.

---

<sup>49</sup> Betænkning nr. 1563/2017, s. 55.

<sup>50</sup> Folketingstidende, Tillæg A, samling 2018-19, L20, s. 46.

<sup>51</sup> Folketingstidende, Tillæg A, samling 2018-19, L20, s. 8.

## 2. Data og datasystemer

§ 263, stk. 1 beskytter henholdsvis *datasystemer* og *data*, som er bestemt til at bruges i et datasystem. Disse udtryk vil i det følgende blive analyseret med henblik på en afgrænsning af bestemmelsens anvendelsesområde.

### 2.1. En andens data, som er bestemt til at bruges i et datasystem

Inden lovændringen i 2018 var beskyttelsesobjektet *oplysninger eller programmer, der er bestemt til at anvendes i et informationssystem*. Det var i den juridiske litteratur antaget, at oplysninger eller programmer måtte forstås som data<sup>52</sup>. Ved lovændringen blev sætningen udskiftet med *data*. Det fremgår af lovforslaget, at denne ændring alene er båret af et forenklingshensyn, hvorfor tidligere forarbejder og retspraksis er således fortsat relevante<sup>53</sup>.

Udvalget har i forbindelse med lovændringen tilkendegivet, at udtrykket *data* ligesom efter hidtil gældende ret skal forstås bredt. Beskyttelsen bør *”ligesom i dag gælde alle former for data, dvs. både programmer, indholdsdata og metadata. Det er således ikke alene indholdet af eksempelvis elektronisk kommunikation, der er beskyttet, men også eksempelvis oplysninger om afsender og modtager af en e-mail, antallet af udvekslede e-mails mellem bestemte personer, størrelsen af vedhæftede filer mv.”*<sup>54</sup>.

Bestemmelsen specificerer, at dataene skal være *en andens*. Det er således uden betydning, om det system gerningsmanden anvender til at tilgå dataene, er sit eget eller en andens. Som et eksempel herpå nævner Straffelovrådet, situationen hvor en udlejer af et datasystem skaffer sig adgang til lejerens data, som er indkodet i datasystemet<sup>55</sup>. I det praktiske liv, er denne sondring særligt vigtig i forhold til cloud lagrings tjenester<sup>56</sup> som f.eks. Dropbox eller OneDrive, hvor brugeren/lejereren mod vederlag kan lagre sine data på udbyderens datasystemer. Her vil der foreligge en overtrædelse af § 263, stk. 1, såfremt udbyderen skaffer sig uberettiget adgang til lejerens indlagte data.

Formuleringen *bestemt til at bruges i et datasystem* tager sigte på, at bestemmelsen også skal omfatte de data, der ikke på gerningstidspunktet indgår i et datasystem, men som er bestemt til at bruges i et datasystem. Hermed sigtes bl.a. til det tilfælde, at en gerningsperson skaffer sig adgang til et USB-stik eller eksternt harddisk. På den anden side vil tilfælde, hvor dataene ikke længere er bestemt til at bruges i et datasystem falde udenfor. Som eksempel herpå nævner Straffelovrådet papirudskrift af data, der har befundet sig, og har været brugt i et datasystem<sup>57</sup>. Det er således uden betydning, om dataene findes online eller offline, om de befinder sig på ikke tilsluttede enheder eller lagringsmedier. Dataene skal blot være bestemt til at bruges i et datasystem. Lars Bo Langsted og Helena Lybæk har anført, at dette led i bestemmelsen medfører, at en uforholdsmæssig stor mængde data vil omfattes af bestemmelsen, da de

---

<sup>52</sup> Toftegaard Nielsen m.fl. – *Kommenteret Straffelov Speciel del*, s. 507 og Lars Bo Langsted – *Strafferettens specielle del*, s. 240 og Lars Bo Langsted m.fl. – *Internetretten*, s. 591.

<sup>53</sup> Folketingstidende, Tillæg A, samling 2018-19, L20, s. 46.

<sup>54</sup> Betænkning nr. 1563/2017, s. 62.

<sup>55</sup> Betænkning nr. 1563/2017, s. 202.

<sup>56</sup> Se mere om cloud baserede tjenester i TfK2013.240.

<sup>57</sup> Betænkning nr. 1563/2017, s. 202.

fleste data på et eller andet tidspunkt benyttes i et datasystem<sup>58</sup>. En for bogstavelig fortolkning af dette led vil føre til, at en person der nærmer sig et stykke papir, og som tror at papiret indeholder oplysninger (data), kunne udløse et strafansvar, såfremt dataene er bestemt til senere at bruges i et datasystem. Der er dog ikke noget der indikerer, at domstolene vil anlægge en så bogstavelig forståelse af bestemmelsen<sup>59</sup>.

Lars og Helena mener derfor, at selv om det ikke fremgår af bestemmelsens ordlyd, bør der indfortolkes et krav om en vis snævrere forbindelse mellem dataene og disses anvendelse i et datasystem<sup>60</sup>.

Data er i Kommenteret Straffelov defineret som: *"enhver form for repræsentation af kendsgerninger eller ideer, der kan kommunikeres eller behandles gennem en eller anden proces. De behøver ikke at være hemmelige eller at berøre følsomme forhold"*<sup>61</sup>.

Cybercrimedirektivet<sup>62</sup> definerer i artikel 2, litra b data 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 et informationssystem til at udføre en funktion"*.

I Budapest konventionen er definitionen på data to-delt, data defineres henholdsvis som *computer data* og *traffic data*. Art. 1, litra b definerer computer data som *"any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"*. Art 1, litra d definerer traffic data som *"any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"*.

Beskrivelserne varierer lidt fra hinanden, men der er det fælles træk, at alle definerer data, som en repræsentation af noget (fakta, informationer, koncepter, osv.), som på en eller anden måde behandles. Uanset hvilken definition der arbejdes efter, er det svært at sige noget konkret om hvad der udgør, eller ikke udgør, data. Ingen af beskrivelserne opsætter en klar grænse, da de er ganske vage. De uklare beskrivelser er nok et resultat af, at det er forsøgt at overføre diffuse IT-begreber til juraen, hvilket i sidste ende blot bidrager til at skabe begrebsforvirring.

Set i lyset af beskyttelsesinteressen, kan det være problematisk både at have en for snæver eller bred definition af data, da bestemmelsen kan komme til at ramme data, som i så fald ikke er beskyttelsesværdige, eller ikke finde anvendelse på data der er beskyttelsesværdige.

Et bredt anvendelsesområde er dog mere hensigtsmæssigt, da det som det vil fremgå endnu ikke findes klart afgrænsede normer på området.

I relation til legalitetsprincippet er det også mindre betænkeligt at have et bredt anvendelsesområde, og i så fald anvende en indskrænkende fortolkning, end at have et for snævert anvendelsesområde, hvor der skal anvendes en udvidende fortolkning eller måske analogislutning.

---

<sup>58</sup> Trzaskowski m.fl. – *Internetretten*, s. 591.

<sup>59</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 178.

<sup>60</sup> Trzaskowski m.fl. – *Internetretten*, s. 591.

<sup>61</sup> Toftegaard Nielsen m.fl. – *Kommenteret straffelov speciel del*, s. 507.

<sup>62</sup> Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013.

## 2.2. Datasystem

Ved indførelsen af § 263, stk. 1 i 1985 skulle de *oplysninger eller programmer* der opnåedes adgang til, være bestemt til at bruges i et *anlæg til elektronisk databehandling*. Som anført af Vagn Greve, fandtes der ikke dengang megen vejledning til forståelsen af begrebet i lovens forarbejder<sup>63</sup>.

I 2004 lovændringen udgik *anlæg til elektronisk databehandling* til fordel for udtrykket *informationssystem*. Om dette udtryk udtaler forarbejderne følgende:

*”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.”*<sup>64</sup>

Som begrundelse for at indføre *informationssystem* anfører forarbejderne, at begrebet er teknologisk neutralt i forhold til de mulige teknologiske løsninger<sup>65</sup>. *Informationssystem* omfatter også mobiltelefoner, intranet og extranet, samt servere, netværk og infrastruktur der udgør internettet<sup>66</sup>.

Straffelovrådet tog i anledning af 2018 revisionen igen terminologien op til fornyet overvejelse. Resultatet af overvejelserne var, at *informationssystem* blev erstattet af *datasystem*. Inden det undersøges, hvad der ligger til grund for denne ændring, skal det her bemærkes, at hvor *informationssystem* forud for 2018 ændringen alene var knyttet til afgrænsningen af de beskyttede *programmer eller oplysninger*, er uberettiget adgang til *datasystemer* nu selvstændig beskyttet.

Hverken betænkningen eller lovforslaget indeholder bemærkninger om de ændringer dette måtte have i hidtil gældende retstilstand. Tværtimod fremgår det af betænkningen at datasystemer som sådan også nød beskyttelse mod uberettiget adgang inden ændringen<sup>67</sup>. Det kan diskuteres om formuleringen indebærer nogen reel ændring, da udtrykket adgang, som det har været anvendt i hidtil gældende ret, forudsætter at gerningspersonen har opnået adgang til datasystemet (se kap. 3, afsnit 4). Det kan være svært at få øje på en situation, hvor den uberettigede adgang ikke er strafbar efter data-leddet, men derimod strafbar efter datasystem-leddet.

Af Straffelovrådets overvejelser fremgår, at begrebet på den ene side er for snævert set ud fra en ordbogsdefinition. På den anden side fandt Straffelovrådet, ud fra en ordlydsfortolkning af de led der indgår i begrebet, at de blot betegner et system til behandling af information. Ordlyden stillede ikke noget krav om, at behandlingen skal ske ved hjælp af en maskine, og dermed rækker begrebet videre end hvad der ligger i straffelovens brug af udtrykket<sup>68</sup>.

---

<sup>63</sup> Greve – *EDB-strafferet*, s. 16.

<sup>64</sup> Folketingstidende, 2003-04, Tillæg A, sp. 1822.

<sup>65</sup> Betænkning 1563/2017, s. 57.

<sup>66</sup> Folketingstidende, 2003-04, Tillæg A, sp. 1822.

<sup>67</sup> Betænkning nr. 1563/2017, s. 56.

<sup>68</sup> Betænkning nr. 1563/2017, s. 57.

Straffelovrådet overvejede bl.a. om terminologien bør ændres henset til Rådets rammeafgørelse 2005/222/RIA, der er indkorporeret i dansk ret ved lov nr. 352 af 19. maj 2004. I dennes artikel 1, litra a bliver informationssystem defineret som: *"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"*.

Straffelovrådet overvejede at indføre udtrykket *enhed eller anlæg til automatisk databehandling*. De anbefalede dog ikke denne formulering, da det ville medføre for tunge sætningskonstruktioner i de bestemmelser som udtrykket indgår i. Indvendingen mod denne formulering begrundes alene med, at *datasystem* er lige så dækkende, men meget simplere. Straffelovrådets bemærkninger til den overvejede formulering er derfor stadig af relevans. De nævner, at medtagelsen af *enhed* ved siden af *anlæg* ville betyde, at også de helt små enheder der i dag behandler data, er omfattet. At ændre *elektronisk* til *automatisk* ville sikre at eventuelle fremtidige automatiserede datasystemer, der ikke benytter elektronisk teknologi ville kunne omfattes<sup>69</sup>. Umiddelbart kan det være svært at få øje på sådanne systemer, der ikke anvender elektronik til behandling af data. All in all bærer Straffelovrådets betragtninger dog præg af et ønske, om at ville fremtidssikre bestemmelsen.

### 3. Uberettiget

#### 3.1. Den uberettigede adgang

Til bestemmelserne § 263-264 d i straffelovens kap. 27 om freds- og ærekrænkelser – herunder hacking - er der indlagt et generelt forbehold om, at handlingen skal have været *uberettiget*. Da § 263, stk. 1. er formuleret i generelle vendinger har bestemmelsen potentielt et meget vidt anvendelsesområde. Begrebet *uberettiget* indtager således en meget central rolle i bedømmelsen af et begået forhold. Der vil derfor blive gjort rede for begrebets baggrund og generelle anvendelse i forhold til hacking. Som det vil fremgå er begrebet meget alsidigt, og anvendelsen kan tage udgangspunkt i en rimelighedstest, samtykke og grundsætningen om materiel atypicitet.

Forarbejderne til lov nr. 229 af 06/07/1985, hvor § 263, stk. 2 blev indført, har defineret det strafbare område således:

*"I lighed med flere af de andre fredskrænkelser vil overtrædelser af den foreslåede bestemmelse bestå i, at en person skaffer sig adgang til noget, der i forhold til ham med rimelighed kan ventes at være et lukket område, det vil sige utilgængeligt. Bestemmelsen omfatter dels den, der som helt udenforstående benytter anlægget (f.eks. ved at tilkoble egen terminal), dels den, der i kraft af et ansættelsesforhold eller som reparatør har lovlige opgaver med hensyn til betjening af anlægget, men går ud over det, som han er bemyndiget til at foretage sig. Hvis den pågældende har tilføjet, ændret eller slettet data eller på anden måde påvirket resultatet af en aktuel eller*

---

<sup>69</sup> Betænkning nr. 1563/2017, s. 58.

*fremtidig retmæssig betjening af anlægget, kan dette være en overtrædelse af en af de senere omtalte bestemmelser, f.eks. om tingsbeskadigelse eller bedrageri.”<sup>70</sup>*

Det ovenfor citerede angiver to typetilfælde, der anses som værende uberettiget, og der afgrænses nogle yderpunkter for den uberettigede adgang. Det første typetilfælde angår den, der som helt udenforstående benytter anlægget. Her omfattes de klassiske tilfælde, hvor gerningspersonen gætter sig frem til, eller benytter et stjålet password, eller bruger deciderede hacker programmer for at skaffe sig adgang til et ikke-offentligt tilgængeligt datasystem. Der skaffes således adgang til et datasystem, som er den pågældende fuldstændig uvedkommende, og derfor er adgangen uberettiget<sup>71</sup>. Det andet typetilfælde angår den, der i kraft af en særlig stilling, eller påhvilende lovlige arbejdsopgaver, opnår en adgang, der går ud over dennes bemyndigelse, hvorved adgangen bliver uberettiget. Det kan dog, som forarbejderne giver udtryk for, forekomme tilfælde, hvor den ansatte har tilgået oplysninger, der ikke har en tilknytning til dennes arbejdsopgaver, men det ikke er sket på en sådan måde, at denne bør straffes<sup>72</sup> (se nærmere herom i kap. 3, afsnit 3.4.).

### 3.1.1. Rimeligheds-testen

Tilbage står det ovenfor citerede *”med rimelighed kan ventes at være et lukket område, det vil sige utilgængeligt”*. Der er med dette udsagn, som påpeget af Helena Lybæk Guðmundsdóttir, lagt op til at der foretages en rimeligheds-test<sup>73</sup>. Betænkningen er fra 1985 og kommer fra en tid, hvor den teknologiske verden så meget anderledes ud. Som påpeget af Lene Wachter<sup>74</sup> og Helena Lybæk Guðmundsdóttir<sup>75</sup>, skal vurderingen af om noget med rimelighed kan ventes at være et lukket område, foretages i lyset af de normer der nu hersker på internettet, herunder at personer deler computere og i stigende grad gør oplysninger tilgængelige for andre. Modhensynet hertil er at ejeren af datasystemet må kunne regulere adgangen og brugen af dette.

I tilfælde hvor der er brudt en sikkerhedsforanstaltning vil adgangen være uberettiget, da det her bør være klart for gerningspersonen, at det han opnår adgang til, med rimelighed måtte forventes at være et lukket område. De tilfælde hvor vurderingen skal anlægges, og hvor denne kan volde tvivl, er hvor der ikke er brudt nogen sikkerhedsforanstaltning, men hvor det uberettigede i stedet kan fremgå af løsere og mere kulturelle barrierer<sup>76</sup>. I sådanne tilfælde kunne det tænkes, at der indgår overvejelser af det indbyrdes forhold mellem personen og ejeren af datasystemet, f.eks. hvor der tidligere har eksisteret et samarbejde, eller hvor personen ud fra et forudgående kendskab til ejeren, kunne have haft en berettiget forventning om, at adgang til datasystemet eller dataene var berettiget<sup>77</sup>. Lars Bo Langsted anfører i tråd hermed, at der i forbindelse med fortolkning af bestemmelserne om fredskrænkelser kan være brug for konkrete interesseafvejninger og

---

<sup>70</sup> Betænkning nr. 1032/1985, s. 25 f.

<sup>71</sup> Trzaskowski m.fl. – *Internetretten*, s. 593.

<sup>72</sup> Betænkning nr. 1032/1984, s. 25f.

<sup>73</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 199.

<sup>74</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 147.

<sup>75</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 199.

<sup>76</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 147.

<sup>77</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 147.

vurderinger, navnlig i tilfælde hvor personen har handlet på baggrund af en særlig relation til ejeren eller en social kutyme<sup>78</sup>.

I de tilfælde hvor adgang til et system kræver et password eller anden kontrol, men hvor systemet i det konkrete tilfælde står åbent, vil det afgørende formentlig være, om der normalvis kræves en adgangskode eller lignende. Som eksempel kan nævnes en computer på et bibliotek, der står tændt og er logget ind på e-boks, skattemapper, e-mail konti, osv. En sådan adgang vil være uberettiget<sup>79</sup>.

Sammenfattende kan siges, at der med begrebet er levnet dommeren vidt rum til at foretage en konkret interesseafvejning og vurdering af om det begåede forhold har været uberettiget. Grænserne for hvad der er berettiget og uberettiget må herefter søges afklaret i retspraksis.

Retspraksis hvor kravet om *uberettiget adgang* er omdrejningspunktet er relativ sparsom, men af relevant praksis kan nævnes **U.2015.345Ø**. Sagen angik T, der via sin computer havde forsøgt at tilgå F's skattemappe og bestilt nyt password til SKAT's hjemmeside. T forklarede i retten, at T ikke ønskede at skaffe sig adgang til F's oplysninger, men blot ønskede at drille F. Herudover oplyste T, at han havde anskaffet F's CPR-nummer igennem en forpagtningskontrakt, som F selv havde lagt op på Facebook.

Byretten fandt, at T's forsøg på at tilgå F's skattemappe ikke var en overtrædelse af daværende § 263, stk. 2, idet F selv havde lagt sit CPR-nummer ud på Facebook. Derimod var det en overtrædelse af daværende § 263, stk. 2 at bestille nye passwords.

Landsretten lagde til grund, at T ad flere gange anvendte F's CPR-nummer på SKAT's hjemmeside, i et forsøg på at tilgå F's skattemappe. Landsretten tilsidesatte T's forklaring om, at han ikke ville skaffe sig adgang til F's oplysninger, og at T havde det til domsfældelse fornødne forsæt. Landsretten mente ikke, at det forhold, at F selv havde lagt sit CPR-nummer ud på Facebook gjorde handlingen berettiget. Landsretten fandt herefter, at T var skyldig i overtrædelse af daværende § 263, stk. 2.

Det indledningsvist mest interessante ved afgørelsen er, at en adgang til et system ikke bliver berettiget ved, at adgangsoplysninger er blevet udleveret af brugeren, hvilket også kan læses ud af *U.2017.2047V & U.2018.1787H*. Hvorvidt adgangen er uberettiget, er altså umiddelbart en mere konkret vurdering, der skal baseres på hvorvidt forurettede ønsker, at holde andre ude fra dette system/program. I relation til skattemapper kan det ikke komme som en overraskelse for en gerningsperson, at forurettede ønsker at holde denne hemmelig.

Denne forståelse er i øvrigt i trit med den generelle beskyttelsesinteresse bag bestemmelserne om fredskrænkelser<sup>80</sup>. Det er altså af mindre relevans hvordan adgangsmidlet de facto er opnået. Det kan, og bør, dog have en betydning, hvordan adgangen er opnået, men som anført af Landsretten, er dette ikke det vigtigste. Dog gælder der en særlig modifikation for medarbejdere, hvilken vil blive gennemgået i næste afsnit.

Dernæst er det interessant, at se på forskellen mellem byrettens og Landsrettens afgørelse. Byretten mente ikke, at begrebet *uberettiget adgang* kunne strækkes til at omfatte tilfælde, hvor gerningsmanden havde fået udleveret adgangsløgin'et, men at det først var uberettiget, når dette login anvendes i et videre omfang,

---

<sup>78</sup> Waaben m.fl. – *Strafferettens specielle del*, s. 236.

<sup>79</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 147.

<sup>80</sup> Betænkning 1032/1985, s. 25.

f.eks. ved at bestille nyt adgangsløgn. Denne forståelse er særligt kritisabel ud fra to henseender. For det første, da det ikke har grundlag i hverken forarbejderne eller litteratur. For det andet, da det ville åbne op for et betydeligt straffrit område. Alle kan komme til at lægge oplysninger på nettet, der kan bruges til at hacke en konto. Hvad hvis jeg gætter en andens adgangsløgn ud fra oplysninger, vedkommende har lagt på internettet, f.eks. navn, alder, første hund osv.?

Landsrettens forståelse af *uberettiget adgang* virker derimod til at være mere i overensstemmelse med forarbejderne og de generelle principper bag fredskrænkelserne.

Når der ovenfor er redegjort for ydergrænserne og vurderingen af om noget med rimelighed må forventes at være et lukket område, kan det passende nævnes, at det i Rådets rammeafgørelse 2005/222/RIA fremgår af præambelns afsnit 13, at det er nødvendigt at undgå overkriminalisering, især af mindre alvorlige tilfælde. Der må således være en bagatelgrænse, hvor der nok er tale om uberettiget adgang til andres data eller datasystem, men hvor tilfældet er af så ringe strafværdighed, at det ikke bør straffes. Hvor denne grænse går er imidlertid svært at sige noget konkret om.

### 3.2. Medarbejdere

Et af de områder som har givet særlig anledning til debat i relation til kravet om *uberettiget adgang*, er de tilfælde, hvor medarbejdere uberettiget tilgår virksomhedens interne datasystemer. Medarbejdere har typisk adgang til interne servere, hvorpå der ligger beskyttelsesværdige data, hvilke de ikke bør tilgå, uden at det har nogen arbejdsmæssig relevans. Det har været op til debat, om det bør ændre ved bestemmelsens anvendelsesområde, at der er tale om en person, der anvender en berettiget adgang på en uberettiget måde.

Forestilles der en person, som har fået adgang til en virksomheds interne dokumenter, f.eks. en IT-chef. IT-Chefen har som en del af sit arbejde behov for at kunne tilgå alle virksomhedens dokumenter, f.eks. for at kunne reparere og genskabe filer. Såfremt IT-Chefen kun tilgår de filer, som er nødvendige for at vedkommende kan udføre sit arbejde, er adgangen berettiget og derfor lovlig. Begynder vedkommende derimod at tilgå filer, som ikke er en del af arbejdet, vil denne adgang være uberettiget, også selvom vedkommende har fuld adgang til dem.

Såfremt § 263, stk. 1 stillede krav om, at en sikkerhedsforanstaltning skulle brydes, ville denne handling ikke umiddelbart blive omfattet af bestemmelsen. Ved derimod at anvende kravet om, at adgangen skal være *uberettiget*, sikres at IT-chefen ikke kan straffes for sit almindelige arbejde, men kan straffes, når filer tilgås uberettiget.

Beskyttelsen mod ansattes uberettigede adgang til data, er der taget højde for ved bestemmelsens udfærdigelse, f.eks. ved at udtrykket *en andens* er bundet op til dataene og ikke dataanlæggene, samt at udtrykket *uberettiget* blev valgt ud fra tanke om, at bestemmelsens brede anvendelsesområde unægtelig ville føre til tilfælde, hvor en handlingens strafbarhed ville afhænge af et konkret skøn fra dommeren<sup>81</sup>. Denne tankegang er videreført i den seneste betænkning fra 2017<sup>82</sup>.

---

<sup>81</sup> Betænkning nr. 1032/1985, s. 26.

<sup>82</sup> Betænkning nr. 1563/2017, s. 58 ff.

Der findes ikke megen trykt praksis om medarbejderes uberettigede adgang, men af relevant praksis kan nævnes *U.1996.979Ø*, *U.2017.3544Ø* og *U.2018.1787*.

I **U.1996.979Ø** havde en bankassistent umiddelbart før sin opsigelse, ved hjælp af sit sædvanlige password skaffet sig adgang til bankens datasystem, hvorefter tiltalte kopierede to af bankens disketter, der blandt andet indeholdt fortrolige oplysninger vedrørende erhvervskunder og bankens hensættelser.

T forklarede, at han foretog handlingen af idioti og kådhed, efter at have følt et nederlag i sit arbejde. T forklare videre, at han hverken ønskede eller kunne bruge oplysningerne til noget i sit nye arbejde. T ville have smidt oplysningerne ud, da han kun ønskede at blære sig.

Byretten fandt, at T's adgang var uberettiget, da der var tale om oplysninger som T ikke ville kunne tilgå efter ansættelsesforholdets ophør, og at T's dispositioner ikke havde en relation til vedkommendes forestående arbejdsopgaver. Retten dømte derfor T for overtrædelse af § 263, stk. 2, jf. stk. 3.

Landsretten lagde til grund for sin afgørelse, at T havde været berettiget til at tilgå oplysningerne, i kraft af sit ansættelsesforhold på gerningstidspunktet. Landsretten frifandt på baggrund af dette T for overtrædelse af § 263, stk. 2.

Dommen er kritiseret af Mads Bryde Andersen i artiklen *Overvågning af medarbejdere og IT-retten*, Gorm Toftegaard Nielsen omtalte den i *U1998.B.270* og senest er den omtalt i betænkning 1563/2017.

Mads Bryde Andersen kritiserer afgørelsen i sin bog. Kritikken angår, at det strider imod bestemmelsens ordlyd og forarbejder, at frikende bankassistenten, på baggrund af at han havde adgang til systemet. Bryde Andersen mener, at dette strider direkte imod bestemmelsens krav om *uberettiget adgang*, da der ikke heri kan fortolkes en undtagelse for personer med et berettiget adgangsløgin<sup>83</sup>.

Som ovenfor nævnt, er der intet krav i bestemmelsen om, at en sikkerhedsforanstaltning skal brydes, overkommes, eller lignende, kravet er derimod blot, at adgangen skal kunne karakteriseres som værende *uberettiget*. Ud fra bestemmelsens forarbejder, må en adgang som den i *U.1996.979Ø* nok siges at være uberettiget, da adgangen ikke har haft noget sammenhæng med den ansattes forestående arbejdsopgaver.

Gorm Toftegaard kritiserer imidlertid, meget kortfattet, Bryde Andersens kritik af *U.1996.979Ø* i artiklen *U.1998B.270/3*. Gorm Toftegaard anser kritikken som værende "*læseværdig*", men mener selv, at Landsretten havde ret, set fra et strafferetligt synspunkt.

Toftegaard har ikke i senere skrifter forklaret, hvad han mener med "*strafferetligt synspunkt*". Toftegaard mener formentlig, at selvom afgørelsen ikke er i overensstemmelse med bestemmelsens ordlyd, er den i overensstemmelse med de grundlæggende strafferetlige synspunkter, hvilke alle straffelovens bestemmelser bør stå til ansvar overfor.

Pointen med at have et straffesystem, er netop at kriminalisere visse former for handlinger, hvilke vi anser som værende uønskede. Pointen med at have en straffelov, er at kunne kodificere visse handlinger som vi som land anser for særligt strafværdige<sup>84</sup>. Set ud fra dette, kan der netop stilles tvivl ved, hvorvidt den handling der er begået i *U.1996.979Ø* er så uønsket, at den bør straffes efter straffeloven, og derved

---

<sup>83</sup> Bryde Andersen – *IT-retten*, s. 746.

<sup>84</sup> Vestergaard – *Strafferetlige Sanktioner*, s. 5 ff.

potentielt medføre frihedsberøvelse. Derimod kan det overvejes, om det vil være mere nærliggende at straffe en sådan handling efter særlovgivning, f.eks. markedsføringsloven eller erstatningsansvarsloven/erstatningsretlige grundprincipper, hvilket i øvrigt også blev anført af forsvareren.

Straffelovrådet kritiserede også Bryde Andersens synspunkt. Det er Straffelovrådets holdning, at dommen ikke skal læses som en endelig afgørelse af, at en berettiget tildelt adgangskode medfører at adgangen herefter altid er berettiget. Dette støtter Straffelovrådet i udtrykket *"efter bevisførelsen"* i dommens præmisser. Hvilket ifølge Straffelovrådet taler imod, at dommen er udtryk for en principiel stillingtagen<sup>85</sup>.

Straffelovrådet udbygger sin holdning med, at der skal anlægges en konkret vurdering af sagens omstændigheder, som også benævnt i 1985-betænkningen. Straffelovrådet mener, at når en medarbejder anvender sit login, kan der lægges vægt på medarbejderens videre forsæt i relation til formålet med at tilgå oplysningerne. Adgangen bør som udgangspunkt anses som værende uberettiget, men i tilfælde hvor medarbejdere tilgår oplysningerne af nysgerrighed, bør domstolene være tilbageholdende med at anse adgangen for at være uberettiget. Rådet mener, at det her vil spille en væsentlig rolle, hvilke oplysninger der faktisk tilgås. Den blotte tilgang til personfølsomme oplysninger, bør dog kunne udgøre en uberettiget adgang i sig selv<sup>86</sup>.

I **U.2017.3544Ø** var T tiltalt for overtrædelse af daværende § 263, stk. 2, ved som ansat i PBS/IBM at have skaffet sig adgang til kreditoplysninger om offentligt kendte personer og udleveret dem til SE og HØR. T havde efter forudgående aftale med ansatte i SE og HØR, tilgået PBS/IBM's interne systemer, herunder systemer vedkommende havde og ikke havde adgang til som en del af sit arbejde. T havde i perioden maj 2008 til primo 2012, skaffet sig adgang oplysninger om ikke under 135 offentligt kendte personer, idet T ikke under 31 gange uberettiget nulstillede andre ansattes adgangskode disses accept eller viden, og herefter i ikke under 67 tilfælde anvende disse ansattes adgang til ikke under 523 gange at søge i kreditkortdatabaser, som T ikke havde en berettiget adgang til. I forbindelse hermed, havde T opnået en uberettiget vinding på ikke under 365.503 kr.

T fandtes at have overtrådt § 263, stk. 3, jf. stk. 2, og blev straffet med fængsel i 1 år og 6 måneder. Herom udtalte Retten, at der var lagt vægt på omfanget og karakteren af det strafbare forhold, herunder at forholdet har strakt sig over en periode på 3½ år, at tiltalte ved sin adfærd groft har forbrudt sig mod den tillid, samfundet skal have til håndtering af systemer til registrering af betalingskort, og at tiltaltes metode medførte en ikke ubetydelig risiko for undersøgelse af andre ansatte.

I lighed med denne dom er **U.2018.1787H**, hvor en tidligere ansat T tre gange som IT-chef havde hacket virksomhedens IT-systemer, og i denne forbindelse slettet data herpå. Dataene kunne genetableres, men angrebene medførte et tab på 400.000 kr. For Højesteret angik sagen, om der var grundlag for at straffe T efter § 263, stk. 3. Herom udtalte Højesteret, at de tre angreb havde et betydeligt omfang og skete indenfor kort tid, med den følge, at virksomheden reelt blev *"lagt ned"*. Højesteret tilsluttede sig Landsrettens udtalelse om, at *"Angrebene er foretaget ved, at tiltalte har udnyttet den viden, som han har fået, mens han havde en betroet stilling i virksomheden. Forholdene henføres på denne baggrund under straffelovens § 263, stk. 3, jf. stk. 2, og § 291, stk. 2"*<sup>87</sup>.

---

<sup>85</sup> Betænkning nr. 1563/2017, s. 60.

<sup>86</sup> Betænkning nr. 1563/2017, s. 61.

<sup>87</sup> U.2018.1787H, s. 1802.

T blev altså ligesom T i U.2017.3544Ø ikke bare straffet for overtrædelse af § 263, stk. 2, men derimod efter den skærpede strafferamme i stk. 3. Der er to afgørende forskelle mellem afgørelserne, for det første at der i U.1996.979Ø var tale om en berettiget adgang, hvorimod der i U.2017.3544Ø og U.2018.1787H var tale om uberettigede adgange. For det andet, at forbrydelsens omfang og skadevirkning var markant større i U.2017.3544Ø og U.2018.1787H.

Det lader til, at det er et vægtigt moment i vurderingen, hvorvidt der er tale om en uberettiget/uautoriseret adgang. Lene Wachter Lentz har fremført det argument, at såfremt medarbejderen i U.2017.3544Ø havde haft en berettiget adgang, ville forholdet ikke være strafbart efter daværende § 263, stk. 2. Hvorvidt dette ville være tilfældet eller ej, er svært at konkludere, det kan blot bemærkes, at i U.2018.1787H var et af T's angreb udført med vedkommendes eget login, dvs. en berettiget adgang, og Højesteret bemærkede intet herom, men statuerede derimod, at de tre angreb skulle vurderes samlet.

I forhold til omfanget, er det tydeligt, at det har en betydning, hvorvidt hackingen har en konsekvens for andre. I U.1996.979Ø havde T ikke forsæt til at anvende oplysningerne til noget, hvorimod T i U.2017.3544Ø og U.2018.1787H netop enten påførte andre et tab enten monetarisk eller personligt. Yderligere har det en betydning, hvorvidt der er tale om en særligt betroet stilling, samt om vedkommende er ansat i en samfundsvigtig virksomhed. Omfanget af forbrydelsen er også særligt relevant i forhold til, hvorvidt handlingen falder ind under den skærpede hjemmel i stk. 3, hvilket vil blive nærmere belyst i kap. 4, afsnit 6.2.

Det lader til, at der er et noget større straffrit område ved medarbejdere, netop da handlingen ofte vil være straffri, såfremt gerningspersonen havde en berettiget adgang. Over for dette står så de tilfælde, hvor gerningspersonen har misbrugt sin stilling i en sådan grad, at handlingen falder ind under stk. 3. Umiddelbart findes ikke praksis, hvor en medarbejder straffes direkte efter stk. 1, hvilket nok skyldes, at der består et betydeligt straffrit område, og at der gælder betinget offentlig påtale for § 263, stk. 1. De tilfælde vi vil se, vil derfor typisk være de meget grove, da virksomhederne sjældent vil anmelde en medarbejder til politiet i mindre grove tilfælde, for at undgå at blive udstillet. Netop af disse grunde, er det særdeles svært, for ikke at sige umuligt, at sige noget konkret om grænsen mellem det strafbare og ustrafbare ved medarbejdere.

### 3.3. Samtykke eller aftale

Der kan gives diskulperende samtykke til handlinger omfattet af §§ 263 og 264<sup>88</sup>, hvilket gør handlingen berettiget. Samtykke skal gives af den, der har rådigheden over den pågældende data/genstand. I relation til hacking er det almindeligt forekommende, at private personer giver samtykke til virksomheder, eller andre private, til at de kan rode rundt i ens data.

---

<sup>88</sup> Bet. Nr. 1563/2017, s. 28 & Lars Bo Langsted – *Strafferettens specielle del*, s. 236.

### 3.4. Materiel atypicitet

I betænkning nr. 601/1971 om privatlivets fred anføres om materiel atypicitet, at man har at gøre med bestemmelser, der har fået en så bred udformning, at der er behov for en regelmæssig udskillelse af handlinger, der anses som værende legale, på trods af at handlingen er omfattet af gerningsbeskrivelsen<sup>89</sup>.

Ud fra den kontekst som udtalelsen indgår i, er der utvivlsomt tale om en reference til princippet om *materiel atypicitet*. I dansk strafferet skal gerningspersonen grundlæggende opfylde 3 betingelser før denne kan pådrage sig strafansvar. Gerningspersonen skal for det første have realiseret et strafbart gerningsindhold jf. § 1. Dernæst skal handlingen eller undladelsen være *retsstridig*. Afslutningsvis skal forholdet subjektivt kunne tilregnes gerningspersonen jf. §§ 15-16 og §§ 19-20<sup>90</sup>. Manglende opfyldelse af retsstridigheds betingelsen kan på den ene side skyldes forekomsten af objektive straffrihedsgrunde, f.eks. nødværge, nødret eller samtykke. På den anden side kan den begåede handling formelt opfylde en bestemmelses gerningsindhold, men i det konkrete tilfælde kan findes atypisk i forhold til lovgivers hensigt med kriminaliseringen. I disse tilfælde er det mest hensigtsmæssigt, og rimeligt, at anlægge en indskrænkende fortolkning. Hermed holdes det konkrete tilfælde uden for det strafbare anvendelsesområde. Dette princip kaldes materiel atypicitet<sup>91</sup>.

Forarbejdernes overvejelser om materiel atypicitet vedrørende krænkelse af privatlivet giver genlyd i betænkning nr. 1032/1985, hvor de udtaler:

*"Ligesom med hensyn til en række andre fredskrænkelser må det anses for nødvendigt at indføre ordet "uberettiget" som led i gerningsbeskrivelsen. Det antydes herved, at der kan forekomme tilfælde, hvor man kun ved et konkret skøn kan afgøre, om en handling, der formelt falder under bestemmelsens ordlyd, skal anses som strafbar. Det nævnte forbehold får næppe nogen praktisk betydning, når det drejer sig om handlinger foretaget af personer, der mangler enhver adgang til at beskæftige sig med det pågældende dataanlæg. For så vidt angår ansatte, vil resultatet være det samme, såfremt den pågældende har benyttet en personlig kode, der ikke tilkommer ham, og på den måde har skaffet sig adgang til oplysninger, der ligger udenfor hans bemyndigelse. Men der kan tænkes grænsetilfælde, hvor den ansatte vel må siges at være gået udenfor sine arbejdsopgaver, men dog ikke på en sådan måde, at han bør straffes. Med henblik på sådanne tilfælde vil ordet "uberettiget" indicere, at der skal anlægges en konkret vurdering af den pågældendes forhold."*<sup>92</sup>

Forarbejderne nævner igen materiel atypicitet i betænkning 1563/2017, men nævner kun at begrebet uberettiget har en nær sammenhæng med princippet, og henviser i øvrigt til forarbejderne fra 1971. 2017 Forarbejderne giver i øvrigt ikke pejlemærker eller vejledning til den praktiske anvendelse af begrebet uberettiget ud fra et synspunkt om materiel atypicitet. Der ses ikke at være praksis, der problematiserer begrebet uberettiget ud fra et synspunkt om materiel atypicitet. Der kan således som Lene<sup>93</sup> har påpeget

---

<sup>89</sup> Betænkning nr. 601/1971, s. 58.

<sup>90</sup> Waaben m.fl. – *Strafferettens almindelige del*, s. 65.

<sup>91</sup> Waaben m.fl. – *Strafferettens almindelige del*, s. 67 & Vestergaard m.fl. – *Forbrydelser og andre strafbare forhold*, s. 4.

<sup>92</sup> Betænkning nr. 1032/1984, s. 25 f.

<sup>93</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 148.

sættes spørgsmålstegn ved, om uberettiget i forhold til materiel atypicitet har fået den funktion som forarbejderne havde tiltænkt den.

Materiel atypicitet finder anvendelse uanset om denne er hjemlet i en bestemmelse eller ej. Når forarbejderne alligevel nævner princippet, må det være udtryk for forarbejdernes erkendelse af bestemmelsernes brede udformning, og at de efter deres art kan omfatte mange forhold. Bemærkningerne i forarbejderne må således anses som en understregning af princippet særlige relevans ved fredskrænkelserne, og et signal til retsanvenderen om, at der i grænsetilfældene må anlægges en meget konkret vurdering, da disse tilfælde kan tænkes at mangle de kendetegn, der karakteriserer den kriminaliserede handling<sup>94</sup>.

### 3.5. Offentlige eller ikke-offentlige data

Straffelovrådet har i betænkning nr. 1563/2017 udtalt sig om betydning af, om data er offentlige eller ikke-offentlige. Som eksempel på offentlige data nævnes, data der kan tilgås igennem en sædvanlig browser, hvilke ikke er beskyttet med en kode eller anden sikkerhedsforanstaltning, det er disse vi kalder offentlige data<sup>95</sup>.

Det er rådets opfattelse, at en tilgang til offentlige data, som udgangspunkt ikke bør anses som værende uberettiget. Dette gælder også, hvis dataene kun kan tilgås ved at gætte sig til en URL, såkaldt URL-hacking (se nedenfor om Topdanmark-sagen). Dette er dog forudsat af, at dataene er blevet gjort tilgængelige ved ejers egen vilje. Er dette ikke tilfældet, kan tilgang til systemet være uberettiget. Det vil imidlertid ofte være svært at statuere et forsæt i en sådan situation<sup>96</sup>.

Ved at indbygge en sondring mellem offentlige og ikke-offentlige data, nærmer dansk ret sig et krav om brud på en sikkerhedsforanstaltning<sup>97</sup>, men på samme tid vil tilfælde, hvor hacking er sket uden at bryde en sikkerhedsforanstaltning fortsat være strafbart.

Som eksempel på et tilfælde, hvor en person havde hacket en virksomhed uden at bryde en sikkerhedsforanstaltning, kan nævnes Topdanmark-sagen<sup>98</sup>. I sagen havde en journalist fra Reuters tilgået Topdanmarks Q1 kvartalsregnskab, forud for at dette var blevet sendt til fondsbørsen. Journalisten kunne tilgå Topdanmarks foreløbige kvartalsregnskab, da Topdanmark havde lagt regnskabet på en server, der kunne tilgås via en almindelig browser, og som ikke var password beskyttet, krypteret, eller lign. Regnskabet kunne imidlertid udelukkende tilgås, såfremt den præcise URL blev indtastet. Regnskabet ville således ikke kunne findes ved at bruge hjemmesidens søgeværktøj.

---

<sup>94</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 198.

<sup>95</sup> Betænkning nr. 1563/2017, s. 62.

<sup>96</sup> Betænkning nr. 1563/2017, s. 63.

<sup>97</sup> Sikkerhedsforanstaltningen består i, at dataene er beskyttet ved, at kun ejeren og indehavere af URL, kan tilgå dataene, såkaldt "security through obscurity".

<sup>98</sup> Topdanmark pressemeddelelse nr. 20/2010 af 07/12/2010.

Sagen endte ikke med retsforfølgelse af Reuters<sup>99</sup>, men den rejser en række interessante problematikker vedrørende hele adgangsbegrebet, særligt i relation til om der er, eller bør være, et krav om brud på en sikkerhedsforanstaltning.

Set i forhold til Straffelovrådets udtaltelse i betænkning nr. 1563/2017, udgør denne handling en interessant grå zone. Straffelovrådet er af den opfattelse, at URL hacking som udgangspunkt ikke er strafbart, men holder alligevel en dør åben i de tilfælde, hvor gerningspersonen er bekendt med, at forurettede ønsker at hemmeligholde oplysningerne<sup>100</sup>.

I dette tilfælde, kan der ikke være tvivl om, at Topdanmarks overførsel til en åben server var en fejl, og at Reuters var bevidste om, at Topdanmark ikke ønskede at offentliggøre regnskabet, særligt da en offentliggørelse forud for fremsendelse til fondsbørsen er i modstrid med de børsetiske regler.

På den anden side står det dog, at oplysningerne er blevet offentliggjort af forurettede.

Lars Bo Langsted udtalte i forbindelse med sagen, at Topdanmarks handlinger kan sammenlignes med at flytte papirer fra en boks til en låst skuffe i virksomhedens kontor. Yderligere udtaltes det, at handlingen ikke udgør en overdragelse af dokumenter fra Topdanmark til journalisten (i relation til børsreglerne), men derimod er der tale om, at journalisten har tilgået hemmelige data gemt på Topdanmarks interne systemer<sup>101</sup>.

Såfremt situationen sammenlignes med at have placeret dokumenter i en aflåst skuffe, er det svært at argumentere imod, at handlingen ikke bør være strafbar efter § 263, stk. 1. Der skal imidlertid gøres to bemærkninger. For det første, er Lars Bo Langsteds udtalelse knyttet op til børsreglerne og ikke den strafferetlige regulering. For det andet, er det særdeles svært at sammenligne data med fysiske dokumenter, grundet datas helt særegne karakter. Det er således svært at give udtalelsen mere vægt, end at den understøtter en forståelse af, at der i et tilfælde som dette, er tale om ikke-offentlige data, eller i hvert fald ikke en offentliggørelse af data.

Sammenfattende kan det siges, at der består tvivl om hvorvidt der er en forskel i at tilgå offentlige eller ikke-offentlige data. Der fremgår intet af bestemmelsens ordlyd, der taler direkte for at skelne mellem offentlige og ikke-offentlige data. Straffelovrådet er derimod af den opfattelse, at der bør gøres forskel mellem offentlige og ikke-offentlige data. Det er imidlertid bare ikke så simpelt at gøre forskel, for i så fald skal det også defineres, hvad der forstås ved offentlige og ikke-offentlige data. Udover eksemplet med Topdanmark, kan der også stilles spørgsmål ved, om det vil have betydning, at der anvendes en modificeret browser for at kunne tilgå data, hvilket eksempelvis er tilfældet med TOR-netværket, da betænkningen bruger udtrykket *sædvanlig webbrowser*<sup>102</sup>. Og det vil også være nødvendigt, at fastsætte hvorvidt der skal gælde visse undtagelser, hvilket Straffelovrådet også selv lægger op til. Der er således nogle betydelige spørgsmål, der skal overvejes, før Straffelovrådets holdning kan blive til retspraksis.

---

<sup>99</sup> Oplyst af Københavns politi.

<sup>100</sup> Betænkning 1563/2017, s. 63.

<sup>101</sup> Topdanmark pressemeddelelse nr. 20/2010 af 07/12/2010.

<sup>102</sup> Betænkning nr. 1563/2017, s. 62.

Straffelovrådet er imidlertid ikke selv kommet med noget særligt konkret, og der er ikke set noget i litteraturen eller retspraksis, der skulle understøtte en sontring. Dog ligger der en vis rimelig i at sige, at en bruger selv er ansvarlig for det vedkommende, lægger på nettet.

### 3.6. Delkonklusion

Begrebet uberettiget skal antageligt ses som et samlet forbehold, der er indsat for at begrænse et ellers bredt anvendelsesområde. Foruden de tilfælde hvor en person klart har overtrådt § 263, stk. 1's anvendelsesområde, f.eks. hvor en udenforstående bryder en sikkerhedsforanstaltning (hvad grænsen for en sikkerhedsforanstaltning er, er dog tvivlsomt) eller medarbejdere der klart overskrider deres bemyndigelse, består der en betydelig gråzone. I disse tilfælde anlægges en rimeligheds-test, hvor der inddrages samtlige relevante momenter. Den sparsomme praksis på området medfører at der stadig består tvivl om hvilke momenter der kan inddrages i vurderingen.

Rimeligheds-testens momenter er mange, men af de mere relevante kan nævnes; sociale normer og kutyper, samtykke/aftale, materiel atypicitet, gerningspersonen relation til forurettede (medarbejder, familie, ven, osv.) og dataene karakter (offentlige/ikke-offentlige, person/virksomhedsfølsomme, osv.)

## 4. Adgangsbegrebet

### 4.1. Introduktion

§ 263 kriminaliserer *adgangen* til data og datasystemer, og der ligger ikke heri et positivt krav om, at der skal have været brudt en form for sikkerhedsforanstaltning, hvilket ellers er et krav i andre EU lande<sup>103</sup>.

Adgang til data kan være på mange forskellige niveauer, en smartphone er godt eksempel herpå. Der er indlagt mange data i en smartphone, herunder data som indehaveren ønsker at hemmeligholde, og visse der ikke er hemmeligholdelsesværdige. Hvis en person (ikke brugeren) tager telefonen op, tænder den og kommer forbi telefonens låseskærm, enten ved at hacke den eller fordi telefonen ikke er password beskyttet, har brugeren nu i princippet adgang til alle data i telefonen, men det er ikke alle data, der er umiddelbart tilgængelige. Visse data vil være gemt et sted i hukommelsen, hvor brugeren ikke uden videre har adgang, f.eks. brugerkonti, kreditkort oplysninger, osv., og der er måske data som indehaveren har beskyttet med password. Spørgsmålet der opstår er, hvor langt ned i et datasystem gerningspersonen skal være trængt, før det kan statueres at denne har opnået adgang?

I betænkning 1417/2002 tilkendegav Brydensholt-udvalget, at der er et problem i at kriminalisere en "*adgang til et informationsystem*". Problemet for udvalget var, at informationssystemer i dag ikke er én "*homogen form*", hvorimod at informationssystemer i 1985 var markant mere simple. Ved ikke at begrænse området,

---

<sup>103</sup> Rapport fra Kommissionen til Europa-Parlamentet Rådet COM(2017) 474, s. 7.

rammer bestemmelsen således et meget bredt udvalg af informationssystemer, herunder systemer som måske ikke påkrævede en beskyttelse<sup>104</sup>.

#### 4.2. Hvornår er der opnået adgang?

Udtrykket *adgang* knytter sig til bestemmelsens fuldbyrdelsesmoment. Af de oprindelige forarbejder til § 263, stk. 1 fremgår, at forbrydelsen er fuldbyrdet når:

*"(...) den pågældende ved tilkobling og betjening af dataanlægget skal have opnået forbindelse til dettes indhold, medens det på den anden side ikke kræves, at han beviseligt har fået kendskab til noget. Det har næppe den største betydning at fastlægge en præcis grænse mellem forsøg og fuldbyrdet forbrydelse. Til strafbart forsøg må henregnes tilfælde, hvor en person, der har forsøgt til at skaffe sig oplysninger, men er ubekendt med en indgangskode, ved sin betjening af dataanlægget kun har opnået at konstatere, at et skærm billede viser en blokering af tilgang til anlæggets indhold. Det er på den anden side en fuldbyrdet overtrædelse, at den pågældende har opnået adgang til andre oplysninger end dem, han er interesseret i"*<sup>105</sup>.

Efter ovenstående beskrivelse er det ikke uden videre klart, hvordan begrebet adgang skal afgrænses. Det kan alene udledes, at gerningspersonen skal have *"opnået forbindelse til dettes indhold"*. Udtrykt lidt anderledes, må dette forstås som, at gerningspersonen har koblet sig på datasystemet, og at dette nu står åbent, hvorefter denne uden mellemkommende skridt kan interagere med de indlagte data. I forbindelse med at gerningspersonen skaffer sig adgang, er det øjensynligt uden betydning, om der de facto opnås kendskab til dataene<sup>106</sup>.

Med hensyn til gerningspersonens forsæt, skal dette være rettet mod at skaffe sig uberettiget adgang. Såfremt gerningspersonen forsøger at opnå adgang, men ikke kan, f.eks. som følge af en adgangskontrol, som den pågældende ikke kender kodeordet til, vil handlingen være strafbar som forsøg<sup>107</sup>. Dette var f.eks. tilfældet i *U.2000.1450Ø*, hvor T ved brug af sin egen pc og et program indlagt på F's PC, forsøgte at skaffe sig adgang, men fejlede pga. tilstedeværelsen af et antivirus program på F's PC.

I dommen i *TfK2017.1034* blev T straffet for forsøg på hacking, ved blot at foretage en scanning for sårbarheder mod hjemmesiden [www.pet.dk](http://www.pet.dk). Selvom gerningspersonen scannede data, der var lagret på en offentlig tilgængelig hjemmeside, skete scanningen med henblik på at finde sårbarheder, og herigennem skaffe sig adgang til ikke-offentlige data.

Da bestemmelsen fuldbyrdes allerede ved opnåelse af adgang, er det således også udtryk for, at kriminaliseringen retter sig mod selve adgangen. Det er altså gerningsmandens mulighed for at kunne interagere med dataene, der er kriminaliseret. Gerningspersonens eventuelle videregående hensigter, eller de følger den uberettigede adgang måtte give anledning til, er som udgangspunkt ikke afgørende i forhold til

---

<sup>104</sup> Betænkning nr. 1417/2002, s. 23 ff.

<sup>105</sup> Betænkning nr. 1032/1985, s. 26 f.

<sup>106</sup> Toftegaard Nielsen m.fl. – *Kommenteret straffelov speciel del*, s. 508 og Lars Bo Langsted – *Strafferettens specielle del*, s. 240.

<sup>107</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 142.

anvendelsen, men kan dog komme til udtryk ved strafudmålingen<sup>108</sup>. De efterfølgende handlinger kan dog udgøre særskilte overtrædelser af straffelovgivningen. Skaffer gerningspersonen f.eks. sig eller andre uberettiget vinding via den uberettigede adgang vil dette alt efter udførelsesmåden kunne udgøre særskilte overtrædelser af §§ 276-279a<sup>109</sup>.

#### 4.2.1. Cybercrime-konventionens adgangs begreb

Danmark har ved lov nr. 352 af 19. maj 2004 inkorporeret Cybercrime konventionen, der i sin artikel 2 pålægger medlemslandene at kriminalisere *hel eller delvis uberettiget adgang til et datasystem*<sup>110</sup>. I forlængelse af konventionen har Europarådet udgivet *Explanatory report to the convention*. Denne indeholder fortolkningsbidrag til konventionens artikler uden at disse fortolkningsbidrag er bindende<sup>111</sup>.

I rapportens afsnit 44 og 46 defineres henholdsvis *ulovlig adgang* og *adgang*, i relation til konventionens artikel 2.

Rapportens afsnit 44 beskriver den ulovlige adgang. Ulovlig adgang er tilfælde, der klart vil være i strid med art. 2. og dermed § 263, stk. 1. Ulovlig adgang defineres som: *"the basic offence of dangerous threats and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data"*. Som eksempler herpå nævner rapporten *hacking*, *cracking* og *computer trespass*, og at disse handlinger i sig selv bør være ulovlige. Hermed er der afstukket et yderpunkt, for hvad der i hvert fald må være uberettiget adgang efter § 263, stk. 1. Opnås adgang således ved deciderede hackerprogrammer eller gennemtrængning af sikkerhedsforanstaltninger, bør kravet om adgang uden videre være opfyldt.

Videre definerer rapporten i afsnit 46 *adgang* som: *"the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content related data). However it does not include the mere sending of an e-mail message or file to that system."* Rapporten nævner endvidere, at typen af forbindelse ikke er afgørende. Der kan således opnås uberettiget adgang uanset om denne sker via internet, intranet eller LAN (local area network).

I tilknytning hertil har Europarådet i Guidance Note 2<sup>112</sup> fastslået, at opnåelsen af adgang til en computer som led i opsættelsen af et *botnet*<sup>113</sup>, vil være uberettiget adgang med hensyn til de computere der inficeres.

Rapporten nævner videre i sit afsnit 48, at når en hjemmeside anvender cookies til at hente oplysninger om brugerens adfærd på hjemmesiden, vil dette indebære adgang til brugerens data.

Det kan således på den ene side anføres, at der til adgang kræves mere en blot tilsendelse af en e-mail. På den anden side, vil deciderede hacking programmer, gæt af passwords mv. konstituere adgang. I spændefeltet herimellem, er vi efterladt med *hel eller delvis adgang til enhver del af et datasystem*. Med hel

---

<sup>108</sup> Betænkning nr. 1563/2017, s. 49.

<sup>109</sup> Betænkning nr. 1563/2017, s. 49.

<sup>110</sup> Vores oversættelse.

<sup>111</sup> Jf. Indledningsordene til rapporten.

<sup>112</sup> T-CY Guidance Note #2 Provisions of the Budapest Convention covering botnets, s. 3 f.

<sup>113</sup> Et botnet er et netværk af computere der er inficerede med malware, der gør det muligt for botmasteren (gerningspersonen), at kontrollere de inficerede computere uden computerens ejers indforståelse, og f.eks. få dem til at udføre DDoS angreb, jf. Jan Trzaskowski m.fl. – *Internetretten*, s. 598.

eller delvis adgang tilkendegives det også, at det ikke er nødvendigt at opnå adgang til hele datasystemet. Det antages også i litteraturen, at gerningspersonen via den adgang der opnås, skal være i stand til at tilføje, ændre eller slette data i systemet<sup>114</sup>.

#### 4.2.2. Kan der opnås adgang, uden at kunne se dataene?

Foruden de tilfælde hvor gerningspersonen klart har opnået adgang til systemet, forekommer der også grænsetilfælde, hvor gerningspersonen uden at være helt inde i datasystemet og kunne se dataene, har interageret med de indlagde data.

Lene Wachter Lentz har beskæftiget sig med dette, og fremkommer i sin artikel<sup>115</sup> med yderligere belysning til forståelsen af adgangsbegrebet. Hun fremhæver Østre Landsrets ankedom af 7. marts 2017<sup>116</sup>, hvor en IT-kyndig far (T), havde brugeradgang til børnehavens kommunikationsplatform. En sikkerhedsbrist i systemet gjorde det muligt for T, at taste programkode i et beskedfelt (script injection). Herved formåede T at ændre i systemets bagvedliggende kode, således at når andre tilgik systemet, fik de vist et pop-up vindue med teksten "*ring til [systemudbyderen] og sig, at jeres nye intranet-løsning er blevet hacket*"<sup>117</sup>.

I byretten blev T dømt for overtrædelse af daværende § 263, stk. 2. Byretten lagde vægt på at T's adgang havde været uberettiget, idet den gik videre end den brugeradgang de andre forældre havde. I Landsretten blev T dog frifundet. Landsrettens vurdering baserede sig på et vidne fra Rigspolitiet, der forklarede, at T ved sin handling ikke havde haft en sådan adgang, at T havde adgang til oplysningerne, eller kunne ændre noget på udbyderens server.

Wachter

Lentz påpeger, at uagtet T ikke fik adgang til de oplysninger, der var indlagt i informationssystemet, herunder oplysninger om børnene, må det antages, at T har opnået adgang til informationssystemets mere tekniske indhold, da T kunne ændre i programmet, der regulerede opsætningen af informationssystemet<sup>118</sup>. T's adgang som bruger antager herefter mere karakter af den adgang, som en administrator har. Wachter Lentz hælder mest til byrettens vurdering, henset til at T i lighed med en administrator har haft mulighed for at låse brugerfladen af med et pop-up vindue, og dermed hindre andre i at tilgå systemet<sup>119</sup>. Lars Bo Langsted og Helena Lybæk Guðmundsdóttir har tillige tilsluttet sig byrettens dom<sup>120</sup>. Det bemærkes dog, at Landsrettens dom ikke forelå på dette tidspunkt.

Til støtte for Landsrettens afgørelse kan det anføres, at T har formået at låse brugerfladen af med et pop-up vindue, men ikke i øvrigt har opnået adgang til oplysninger på systemudbyderens server. T har altså ikke kunne se den bagvedliggende programkode, der dikterer databehandlingen på systemet. Bestemmelsens beskyttelsesinteresse består i, at andre ikke skal kunne snage i en persons eller virksomheds oplysninger.

---

<sup>114</sup> Karnovs note 1281 til § 263, stk. 1 (senest tilgået 16. maj 2019)

<sup>115</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 149.

<sup>116</sup> S-2696-16, forfatterne har forsøgt at få et udskrift af dommen, hvilket imidlertid ikke er lykkedes.

<sup>117</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 149.

<sup>118</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 149.

<sup>119</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 149.

<sup>120</sup> Trzaskowski m.fl. – *Internetretten*, s. 598, fodnote 56.

Dette er da heller ikke tilfældet i den foreliggende sag. T har uden at kunne se programkoden kunne indskyde ny programkode. Der foreligger således ikke umiddelbart en uberettiget adgang, derimod vil det kunne overvejes om handlingen kunne straffes som hærværk, jf. § 291.

Denne antagelse støttes i øvrigt af CSC-sagen<sup>121</sup>, der blev afsagt omkring samme tidspunkt. Her fik de tiltalte adgang til oplysninger, der lå på CSC's mainframe. Men herudover oprettede de tiltalte tre bagdøre, ved at oprette et script i systemet, og ved at ændre i to konfigurationsfiler. Selve adgangen blev straffet jf. § 263, stk. 2, mens oprettelsen af bagdørene blev straffet som groft hærværk jf. § 291, stk. 2.

#### 4.3. Kriminalisering af en hypotetisk mulighed?

I henhold til den originale betænkning, skal begrebet *adgang* altså forstås meget bredt, men som tidligere nævnt må et adgangsløgin udgøre den ydre grænse. Da lagringssystemer i dag er ganske komplekse, kan det dog virke ganske uholdbart, at sætte grænsen ved et adgangsløgin eller lignende foranstaltning.

Skeles der til § 263, stk. 2, nr. 1, ligger der et krav om, at meddelelsen skal være *åbnet* eller *unddraget*. Bestemmelsen kriminaliserer altså ikke alene muligheden for at gøre sig bekendt med indholdet i en lukket meddelelse, derimod ligger der et krav om, at gerningsmanden skal have gjort noget aktivt. Ligesom i § 263, stk. 1 ligger der dog ikke et krav om, at gerningsmanden faktisk er blevet bekendt med indholdet af meddelelsen<sup>122</sup>.

Det kan således virke lidt besynderligt, at § 263, stk. 1 kriminaliserer den simple mulighed for at gøre sig bekendt med data. Umiddelbart virker det mere logisk, at følge samme tilgang som i § 263, stk. 2, og indlægge et yderligere krav i form at gerningsmanden har foretaget en faktisk handling med henblik på skaffe sig et indblik i dataene.

Det er endvidere diskutabelt, hvorvidt den teoretiske forståelse af adgangs-begrebet er helt i overensstemmelse med den faktiske anvendelse.

I **AM2018.09.26Ø** var T tiltalt for overtrædelse af §§ 264 d, 232 og 263, stk. 2 (i dag stk. 1), ved gentagende gange at have skaffet sig adgang til F1-6's data, blandt andet igennem personlige e-mails, e-boks, personaleIntra-profil, Facebook-konti samt computere. I alle tilfælde af indtrængen, har T foretaget enkelte handlinger, f.eks. slettet mail, kopieret bestemte data eller taget screenshots af noget bestemt.

Anlægger vi den forståelse af *adgang*, som både den oprindelige betænkning og kommenterede straffelov har fremsat<sup>123</sup>, burde T blive straffet for at have skaffet sig adgang til alle de oplysninger, som var tilgængelige på de respektive databaser T havde tilgået, uanset om han kun var interesseret i visse oplysninger. Anklagemyndighedens opgave burde i så fald udelukkende være, at bevise en indtrængen i systemet.

Afgørelsen går imidlertid i en anden retning. T blev dømt for overtrædelse af §§ 264 d, 232 og daværende 263, stk. 2. I relation til § 263, stk. 2 dømtes T ikke for at have skaffet sig adgang til alle oplysninger, som han reelt havde mulighed for at tilgå, derimod blev T kun straffet for de oplysninger, som Anklagemyndigheden kunne bevise, at T de facto havde skaffet sig adgang til, f.eks. ved at have slettet dataene eller overført dem

---

<sup>121</sup> U.2015.3615Ø.

<sup>122</sup> Toftegaard Nielsen m.fl. – *Kommenteret straffelov speciel del*, s. 504.

<sup>123</sup> Toftegaard Nielsen m.fl. – *Kommenteret straffelov speciel del*, s. 508.

til sit eget lagringsmedie. Anklagemyndigheden skulle således ikke blot bevise en indtrængen på systemet, men derimod en konkret handling foretaget i systemet, hvilken T blev straffet for.

Måden hvorpå adgangsbegrebet er beskrevet i teorien, lader ikke til at have taget højde for den praktiske anvendelse. Det virker umiddelbart mest logisk kun at straffe for adgang til data, som gerningsmanden beviseligt har tilgået. Såfremt vi anvender den modsatte tankegang, straffes gerningsmanden for en hypotetisk mulighed for at tilgå visse data, og ikke gerningsmandens faktiske handlinger/forsæt.

Antages den situation, at en gerningsperson uberettiget skaffer sig adgang til en andens PC, hvor gerningspersonen kun er interesseret i at skaffe sig kreditkortoplysninger, men der så også ligger andre personfølsomme oplysninger. Hvor meget skal der i så fald til for at kunne statuere, at gerningsmanden også har skaffet sig adgang til de personfølsomme oplysninger? Er det den blotte mulighed eller skal vedkommende have gjort noget mere konkret?

En forståelse af adgang som der er lagt op til i forarbejderne bærer tydeligt præg af markant simple lagringssystemer. Uanset hvad der står i forarbejderne og den kommenterede straffelov, virker det mest formålstjenstligt, at antage *adgang* som værende en faktisk adgang og ikke en teoretisk, hvilket umiddelbart også er den måde som bestemmelsen anvendes i praksis.

## 5. Betinget offentlig påtale

Det følger af § 275, stk. 2, nr. 1, at der for hacking gælder betinget offentlig påtale. Anklagemyndigheden kan således kun påtale en strafbar overtrædelse af § 263, stk. 1, såfremt begæring herom fremsættes af en hertil berettiget jf. retsplejelovens § 720, stk. 2, 1. pkt. Den berettigede vil typisk være den forurettede jf. retsplejelovens § 725, stk. 1. Strafferetlig forfølgning af en gerningsperson, vil således være under forurettedes råden. På baggrund af påtalereglerne har retspraksis været sparsom og klarlægningen af hacking bestemmelsens anvendelsesområde i nogen grad hindret. Men med den stigende opmærksomhed på hacking – både på nationalt og internationalt plan – kunne det tyde på en vis opblødning.

Foruden at der som ovenfor anført, har været en tilbageholdenhed med at anmelde tilfælde af hacking, da virksomheder risikerer at udstille sig selv som ikke havende styr på IT-sikkerheden, har Trine Baumbach påpeget et stort og påtrængende problem. I nutidens samfund bliver personoplysninger om stort set alle aspekter af borgerens liv samlet i registre. Det er derfor overordentlig vigtigt, at borgerne har tillid til at disse registre ikke misbruges af uvedkommende. Samfundet kan ikke forvente, at borgerne lader sig indregistrere, hvis samfundet ikke samtidigt har et effektivt og retshåndhævende apparat, der retsforfølger hacking og forsøg herpå. I modsat fald kan det gå ud over borgernes tillid til myndigheder og borgere indbyrdes. Der er således mere på spil, end blot den enkelte forurettedes syn på det konkrete tilfælde af hacking<sup>124</sup>.

---

<sup>124</sup> Baumbach – *I forskningens og formidlingens tjeneste – Hacker bestemmelsen, Se og Hør-sagen og nyere tendenser*, s. 27-28.

## 6. Strafferammen i § 263, stk. 1

### 6.1. Normalstrafferammen

Strafferammen i § 263, stk. 1 er i dag fængsel indtil 1 år og 6 måneder. Straffen var indtil 2004 fængsel indtil 6 måneder. Forhøjelsen skyldes ifølge forarbejderne, at det IT-baserede samfund i dag er sårbart. Selv om hacking kan medføre store omkostninger til kontrol af systemet og evt. midlertidig driftsstandsning, betegner forarbejderne det dog som en normalsituation, og ikke en specialsituation der omfattes af den skærpede strafferamme i stk. 3<sup>125</sup>. Straffelovrådet foreslog derfor en strafferamme på 1 år og 6 måneder, så forbrydelsens indgribende karakter også afspejles i den ikke kvalificerede bestemmelse.

Efter denne forhøjelse i strafferammen er det i dag mere strafbart, at skaffe sig uberettiget adgang til data på et datasystem, end det er at skaffe sig adgang til oplysninger f.eks. i et brev eller andre optegnelser (stk. 2). Denne ulighed i strafferammen understreger forbrydelsens alvor i et hurtigt udviklende digitalt samfund.

### 6.2. Skærpende omstændigheder

§ 263, stk. 3 indeholder den skærpede strafferamme for hacking, der udvider straffen til fængsel indtil 6 år. Efter ordlyden vil skærpende omstændigheder foreligge 1) hvor gerningspersonen skaffer sig eller gør sig bekendt med en virksomheds erhvervshemmeligheder 2) eller hvor handlingen begås *under andre særligt skærpende omstændigheder* eller 3) når der er tale om overtrædelser af mere systematisk eller organiseret karakter.

Forarbejderne udtrykker, at det kan være svært at sige noget konkret om *andre særligt skærpende omstændigheder*. De nævner dog samtidig at de har tænkt på situationer hvor udnyttelse eller videregivelse af oplysninger medfører betydelige skadevirkninger, f.eks. ved adgang til offentlige edb-registre<sup>126</sup>. Fra praksis kan nævnes U.2017.3544Ø, hvor T opnåede uberettiget adgang til systemer til registrering af betalingskort. Landsretten lagde her vægt på, at T groft har forbrudt sig mod den tillid som samfundet skal have til sådanne systemer. Endvidere kan nævnes U.2018.1787H, hvor Højesteret lagde vægt på, at angrebene var sket ved benyttelse af den viden, T havde opnået i kraft af sin betroede stilling, samt angrebet omfang og skadevirkning (400.000 kr. + tabt arbejdsfortjeneste).

For så vidt angår strafskærpelse som følge af forholdets systematiske eller organiserede karakter kan nævnes TfK2017.1034, hvor T havde blev dømt for at have opnået uberettiget adgang til dele af Socialistisk Folkepartis medlemsregister og foretaget scanninger af 26 hjemmesider, hvilket Retten fandt, var systematisk og organiseret hacking og derfor omfattes af stk. 3.

Herudover kan U.2018.1787H igen benævnes. T havde inden for kort tid udført 3 separate hackerangreb mod det samme mål, hvorfor Højesteret fandt, at angrebene skulle vurderes samlet. Det er der tale om separate angreb er altså ikke nok til at statuere, at angrebene var *systematiske* eller *organiserede*. Derimod skal det indgå som moment, om der er tale om forskellige mål og den tidsmæssige sammenhæng mellem angrebene.

---

<sup>125</sup> Betænkning 1417/2002, s. 75 og Folketingstidende, Tillæg A, samling 2003/04, sp. 1774.

<sup>126</sup> Betænkning nr. 1417/2002, s. 75.

Retspraksis er fåtalligt, og hverken forarbejderne eller litteraturen er særligt konkrete i deres beskrivelser af anvendelsesområdet. Der er således ikke mange pejlemærker for hvornår en gerning falder ind under stk. 3, hvilket også tydeligt ses i de nævnte afgørelser. Dog er det muligt at kunne udstikke visse momenter som værende af betydning, herunder typen af stilling, skadens omfang og antallet af angreb som de mere vægtige.

## 7. Grundlæggende strafferetlige principper, menneskerettighederne og hacking

Individet er igennem både dansk ret og folkeret tildelt rettigheder, der skal sikre at deres handlinger og undladelser kun straffes, når den lovgivende magt har villet det. I Straffeloven er beskyttelsen kodificeret i § 1, og for så vidt angår internationale forpligtelser er princippet kodificeret i Menneskerettighedskonventionens artikel 7.

Som det er fremgået af de forudgående afsnit, er hacking bestemmelsen formuleret i generelle vendinger, og har efter sin ordlyd et meget bredt anvendelsesområde. I det følgende analyseres § 263, stk. 1 overensstemmelse med disse strafferetlige principper.

Afsnit 7.1. undersøger § 263, stk. 1 i forhold til det danske strafferetlige legalitetsprincip og afsnit 7.2. undersøger § 263, stk. 1 ud fra menneskerettighedskonventionens artikel. 7.

### 7.1. Straffelovens legalitetsprincip

Da straffelovens legalitetsprincip som det vil fremgå, indebærer en begrænsning i den almindelige fortolkningslæres udgangspunkt, gives der indledningsvis et kort indblik i den almindelige fortolkningslære.

#### 7.1.1. Fortolkningslæren

Den almindelige fortolkningslære sonderer overordnet mellem tre fortolkningsvarianter når fortolkningen vedrører en afgørelses resultat. Disse tre er: præciserende, udvidende og indskrænkende fortolkning. Den almindelige fortolkningslære sonderer endvidere mellem subjektiv og objektiv fortolkning. Disse to sidste fortolkningsvarianter refererer til en afgørelses præmisser. Den præciserende fortolkning indebærer at der ud fra bestemmelsens ordlyd, vælges den fortolkning der gør bestemmelsen mere præcis, og derfor en fortolkning der stadig kan rummes inden for bestemmelsens sproglige ramme. Den indskrænkende fortolkning indebærer at et forhold der umiddelbart falder ind under bestemmelsens ordlyd holdes uden for anvendelsesområdet. Modsat inddrager den udvidende fortolkning forhold der umiddelbart ikke er omfattet af bestemmelsens ordlyd ind under dennes anvendelsesområde<sup>127</sup>. Anvendelsen af udvidende og indskrænkende fortolkning indebærer altid at retsanvenderen sætter sig ud over bestemmelsens ordlyd. Anvendes et af disse to fortolkningsprincipper, andrager fortolkningen retspolitisk karakter, da

---

<sup>127</sup> Baumbach – *Strafferet og menneskeret*, s. 74-76.

retsanvenderen ved enten at inddrage, eller udelukke forhold der i forhold til ordlyden vil være omfattet eller ikke omfattet bevæger sig ind på lovgivers område<sup>128</sup>.

### 7.1.2. Straffelovens § 1

Der findes som udgangspunkt ikke nogen begrænsning for den udvidende fortolkning i dansk ret, men af § 1, 1. pkt. fremgår det, at:

*”Straf kan kun pålægges for et forhold, hvis strafbarhed er hjemlet ved lov, eller som ganske må ligestilles med et sådant.”*

Efter § 1, kan der kun pålægges straf for et begået forhold, hvis det begåede forhold enten direkte kan omfattes af straffebestemmelsens ordlyd, eller hvis det begåede forhold *ganske* kan sidestilles med et forhold der direkte omfattes af bestemmelsens ordlyd<sup>129</sup>.

Legalitetsprincippet begrænser den udvidende fortolkning til alene at tillade analogi i tilfælde hvor det begåede forhold ganske må ligestilles med et forhold der er omfattet af ordlyden. Dette kaldes også en analogibegrænsning, da analogi forstås som lighed i forhold<sup>130</sup>. Begrænsning er en undtagelse til den almindelige fortolkningslæres regler om udvidende fortolkning. Omvendt indeholder § 1 udtrykkelig hjemmel til begrænset udvidende fortolkning<sup>131</sup>.

Tanken bag legalitetsprincippet er retfærdighedstanken om, at det lige skal behandles lige. Legalitetsgrundsætningen udgør borgerens værn mod vilkårlighed<sup>132</sup>. Den sikrer at borgerens handlinger og undladelser kun er strafbare, når den lovgivende magt har villet det, og at borgere kan opnå en indsigt i hvilke handlinger og undladelser kan straffes<sup>133</sup>.

Lars Bo Langsted har fremhævet nogle vigtige punkter om legalitetsprincippet man bør være opmærksom på, når straffelovens bestemmelser anvendes og deres grænser bestemmes. Et af disse punkter er, at beskyttelsestankerne bag § 1 ikke opfyldes ved at tilvejebringe en hjemmel til straf efter at en handling er begået, men inden dom afsiges. For at beskyttelsestankerne bag § 1 opfyldes, kræves at bestemmelserne kan indgå i borgerens beslutningsgrundlag inden denne foretager en handling. Lars fremhæver endvidere at det for § 1 ikke er en holdbar forudsætning at borgerne faktisk studerer og gør brug af loven som led i deres beslutningstagen. Dog er det grundlæggende nødvendigt at borgeren, såfremt denne ønsker at studere og inddrage loven, har mulighed for at kende lovgivers standpunkt<sup>134</sup>.

Der kan netop stilles spørgsmål ved, om § 263, stk. 1 faktisk afspejler hvordan borgere generelt agerer, således at borgere kan fortage deres daglige gøren og laden, i overensstemmelse med de kulturelle kutyper. Noget kunne tyde på, at dette i dag ikke er tilfældet, særligt med udbredelsen af sociale medier og teknologi.

---

<sup>128</sup> Baumbach – *Strafferet og menneskeret*, s. 76.

<sup>129</sup> Baumbach – *Strafferet og menneskeret*, s. 78.

<sup>130</sup> Baumbach – *Strafferet og menneskeret*, s. 78.

<sup>131</sup> Baumbach – *Strafferet og menneskeret*, s. 79.

<sup>132</sup> Baumbach – *Strafferet og menneskeret*, s. 78.

<sup>133</sup> Bo Langsted – *Strafferettens almindelige del*, s. 91.

<sup>134</sup> Bo Langsted – *Strafferettens almindelige del*, s. 92f.

Som Lars Bo Langsted dog videre konkluderer, gælder der nok ikke i dansk ret en generel grænse for hvor brede eller uklare ordvalg lovgiver kan gøre brug af. Derimod må det af hensyn til respekt for domstolenes kompetence siges, at være formålstjenstligt at anvende ord der kan fortolkes en smule på. På samme tid vil det være usandsynligt, at en domstol vil tilsidesætte en lov på baggrund af, at den er for uklar<sup>135</sup>. Denne holdning er i øvrigt understøttet af den eksisterende praksis.

I **U.1989.688H** var handlingen i strid med forarbejderne, men ikke bestemmelsens ordlyd, og i **U.1995.405V** var der tale om en uklar bødehjemmel i RPL § 185, stk. 1, 1. pkt. jf. § 1015, stk. 2. I begge afgørelser tilsidesatte domstolene ikke lovgivningen som sådan, men konkluderede derimod, i overensstemmelse med eksisterende fortolkningsprincipper, at de tiltalte handlinger ikke er omfattet af bestemmelsernes anvendelsesområde. Den samme tilgang ses i øvrig domspraksis<sup>136</sup>. En dommer skal såfremt denne efter fortolkning af bestemmelsen, finder det tvivlsomt om et forhold udgør en realisation af et bestemmelses gerningsindhold, frifinde den tiltalte. Frifindelsen skyldes i så fald den manglende hjemmel, og er således ikke udtryk for, at der gælder et krav om klarhed<sup>137</sup>.

Baggrunden for at der ikke gælder et krav om klarhed er, at der på lovgivningsplan allerede eksisterer hjemmel til begrænset udvidende fortolkning i § 1. Den mere praktiske begrundelse er, at bestemmelser næsten uden undtagelse, må underkastes fortolkning før de kan anvendes. Endvidere vil det være en umådelig svær opgave for lovgiver at udforme en bestemmelse, der på samme tid er præcis, dækkende og tager højde for alle tænkelige tilfælde. Et krav om klarhed til en bestemmelses ordlyd, må derfor henregnes til retningslinjer for god lovgivningsskik og retspolitiske diskussioner<sup>138</sup>.

## 7.2. Den Europæiske Menneskerettighedskonvention

Den Europæiske Menneskerettighedskonventions indeholder i sin art. 7. i lighed med § 1 tillige et strafferetligt legalitetsprincip. Artikel 7, stk. 1, 1. pkt. er sålydende:

*"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."*

Artikel 7 indeholder grundlæggende det samme legalitetsprincip som § 1. Vedrørende udstrækningen af begrebet *ret/law* er dette dog lidt bredere, end det er efter § 1. Menneskerettighedsdomstolen (Domstolen) har herom udtalt:

*"In this connection, the Court has always understood the term law in its substantive sense, not its formal one. It has thus included both enactments of lower rank than statutes and unwritten law ... In sum, the law is the provision in force as the competent courts have interpreted it"*<sup>139</sup>

---

<sup>135</sup> Bo Langsted – *Strafferettens almindelige del*, s. 93.

<sup>136</sup> Se f.eks. U1969.56, U1991.85H, U1992.16V og 1997.634.

<sup>137</sup> Baumbach – *Strafferet og menneskeret*, s. 122.

<sup>138</sup> Baumbach – *Strafferet og menneskeret*, s. 122.

<sup>139</sup> *Kafkaris v. Cyprus* (app.no. 21906/04), dom af 12. februar 2008, pr. 139.

Retsbegrebet efter artikel 7, omfatter således ikke blot en egentlig vedtaget lov, men også uskrevne retsgrundsætninger, og bestemmelser som de kompetente domstole har måtte fortolke den. Da der ikke i art. 7 henvises direkte til en legislativ bestemmelse, er det afgørende om retsgrundlaget var tilgængeligt for borgeren, og om retstilstanden er forudsigeligt<sup>140</sup>.

Domstolen har i dommen *Kokkinakis v. Greece* udtalt følgende om legalitetsprincippet i artikel 7:

*"The Court points out that Article 7 para. 1 (art. 7-1) of the Convention is not confined to prohibiting the retrospective application of the 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."*<sup>141</sup>

En forbrydelse skal altså være klart defineret i loven. Det følger samtidig heraf, at denne betingelse er opfyldt, såfremt den endelige fortolkning af det relevante retsgrundlag, herunder praksis, og ved hjælp af juridisk bistand er forudsigelig<sup>142</sup>.

Hacking bestemmelsen er bredt og vagt formuleret. Men hvordan klarer den sig i relation til forudsigelighedsvurderingen efter artikel 7?

Af praksis fra Domstolen der relaterer sig til forudsigelighedsvurderingen, kan nævnes sagen *Schimanek v. Austria*<sup>143</sup> hvor Domstolen udtalte, at en bestemmelse der *"appears rather vague"*, ikke er en hindring for idømmelse af straf, såfremt det er muligt fastlægge retstilstanden. I en anden sag *Wingrove v. the United Kingdom*<sup>144</sup>, fandt Domstolen, at det ikke udgjorde en krænkelse af artikel 7, at to journalister blev pålagt straf efter en straffebestemmelse, der kriminaliserede krænkelse af privatlivet. Domstolen fandt også begrebet uklart, men på trods heraf lagde Domstolen vægt på, at det for de domfældte journalister bl.a. ud fra bestemmelsens forarbejder, retspraksis mv. havde været muligt at forudse de strafferetlige følger af deres handlinger, evt. efter opsøgt rådgivning.<sup>145</sup>

Tvivl om en bestemmelse der kan tilskrives, at der i praksis findes en gradvis udvikling af bestemmelsens anvendelsesområde - herunder i retspraksis - udgør ikke en krænkelse af de kvalitative krav, der følger af artikel 7<sup>146</sup>. For at en sådan gradvis retsudvikling ikke skal udgøre en krænkelse, er det dog et krav, at udviklingen er forenelig med forbrydelsens væsen, og at udviklingen med rimelighed kan forudses<sup>147</sup>.

---

<sup>140</sup> Baumbach – *Strafferet og menneskeret* s. 130.

<sup>141</sup> *Kokkinakis v. Greece*, app no. 14307/88, præmis 52.

<sup>142</sup> Baumbach – *Strafferet og menneskeret*, s. 142.

<sup>143</sup> App. No. 32307/96 afgørelse af 1. februar 2000.

<sup>144</sup> App. No. 17419/90 afgørelse af 25. november 1990

<sup>145</sup> Baumbach – *Strafferet og menneskeret*, s. 143.

<sup>146</sup> Baumbach – *Strafferet og menneskeret*, s. 146.

<sup>147</sup> Baumbach – *Strafferet og menneskeret*, s. 146.

Denne balance mellem, på den ene side, de kvalitative krav artikel 7 stiller til en straffebestemmelse, og på den anden side, at de nationale domstole ved udvidende fortolkning kan udvide de allerede eksisterende straffebestemmelser anvendelsesområde, må siges at være hensigtsmæssig. Det forekommer undertiden at straffebestemmelser er bagud i forhold til den teknologiske udvikling. § 263, stk. 1 befinder sig i praksis netop i en sådan situation. Art. 7 udgør således ikke en hindring for, at bestemmelser som § 263, stk. 1 fortsat finder anvendelse på nye tilfælde f.eks. grundet nye teknologiske tider, men sikrer at bestemmelser som § 263, stk. 1 fortsat kan udgøre en effektiv beskyttelse for borgere mod overgreb fra gerningspersoner, der qua udviklingen har opdaget nye veje til overgreb. Domstolen er indforstået med, at straffebestemmelser i langt de fleste tilfælde, må underkastes fortolkning for at finde anvendelse<sup>148</sup>. Dog gælder den udvidende fortolkning ikke undtagelsesfrit, idet den i alle tilfælde med rimelighed skal kunne forudsiges.

### 7.3. Delkonklusion

Det er intet som peger på, at § 263, stk. 1 skulle være i modstrid med § 1 eller Den Europæiske Menneskerettighedskonvention art. 7, men uanset at dette nok ikke er tilfældet, kan der ikke ses bort fra, at lovgiver ved udøvelse af sin lovgivningskompetence, bør være bevist om strafferettens idealer, herunder at den strafferetlige regulering bør være klar og afspejle sig i den gældende kultur.

Lovgiver bør altid tilstræbe, at skabe så klare bestemmelser som muligt. Undertiden er dette dog en meget svær opgave. Særligt svært bliver det på et område, som stadig er meget nyt. Som Helene Lybæk Guðmundsdóttir har påpeget, har vi i den fysiske verden haft hundredevis af år til at udforske grænserne mellem det acceptable og det uacceptable ift. privatlivets fred. Med introduktionen af internettet kan disse normer ikke direkte overføres, og som samfund er vi igen nødt til at udforske grænserne<sup>149</sup>. Når man som samfund befinder sig i en sådan fase, kan lovgiver være nødsaget til at udforme bestemmelsen om hacking bredt og måske efter noget tid, når grænserne er ved at tegne sig, tage bestemmelsen op til revurdering.

Bestemmelsens uklarhed er desuden også et resultat af de påtaleregler, der gælder, da disse har stor indflydelse på hvilke sager der kommer for en domstol, og dermed også bestemmelsens klarlæggelse i retspraksis.

---

<sup>148</sup> Baumbach – *Strafferet og menneskeret*, s. 151.

<sup>149</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 199.

## Kapitel 4

Selvom ret overordnet set er et nationalt anliggende, er det stadig relevant at se på, hvilke retskilder der findes uden for dansk ret.

Hacking, og cybercrime generelt, er en meget international kriminalitetsform, hvorfor det er særligt relevant at kende retsstillingen i andre lande, herunder særligt lande som ligger os nær, både geografisk og retligt. Det er trods alt lidt mere besværligt for mig fysisk at røve en bank i Rom, end en her i Aalborg, men det er fuldstændig irrelevant for mig, om jeg hacker et datasystem beliggende i Aalborg eller Rom. Jeg har endda et incitament til at gøre det i Rom, da dette vil besværliggøre efterforskningen.

Netop derfor er det relevant, at lande finder et vist fælles retligt ståsted, så der sikres en gennemgribende og ensrettet kriminalisering af cybercrime, herunder hacking. De forskellige internationale retskilder behandler selvfølgelig mere end blot hacking, men da projektet er begrænset til hacking, vil vi kun se på de dele der er relevante hertil.

Som anført i kap. 2, afsnit 3.3 er Cybercrime direktivet ikke en del af dansk ret. Direktivet er imidlertid bindende for de øvrige 27 EU-medlemslande<sup>150</sup>. For at kunne få et billede af den gældende retsstilling i de øvrige EU-lande, er det således relevant at behandle direktivet.

### 1. Cybercrime direktivet

#### 1.1. Direktivets genstand

Direktivet er et minimumsdirektiv, der fastsætter minimumsregler om kriminelle handlinger og sanktioner herfor i relation til angreb på informationssystemer. Herudover søger direktivet at forbygge sådanne handlinger, og forbedre samarbejdet mellem medlemsstaternes kompetente myndigheder.

Da direktivet er et minimumsdirektiv, er der ikke noget i vejen for, at medlemsstaterne indfører regler der går længere end direktivet foreskriver. Medlemsstaterne vil således kunne opfylde direktivets krav om kriminalisering af bestemte handlinger ved en mere generel kriminalisering.

#### 1.2. Direktivets definitioner

Direktivets artikel 2 definerer 4 begreber, hvilke anses som værende af særlig vigtig betydning: *Information system (informationssystem)*, *computer data (edb-data)*, *legal person (juridisk person)* og *without right (uretmæssig)*.

Definitionerne svarer, med visse mindre sproglige præciseringer, til definitionerne i Rådets rammeafgørelse 2005/222/RIA.

Ved *informationssystem* forstås, "enhed eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program, som automatisk behandler edb- data, samt edb-data, som

---

<sup>150</sup> Rapport fra Kommissionen til Europa-Parlamentet og Rådet COM(2017) 474, s. 5.

*lagres, behandles, fremfindes eller overføres af denne enhed eller gruppe af enheder i forbindelse med dens eller deres drift, brug, beskyttelse og vedligeholdelse”.*

*Ved edb-data forstås, ”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 et informationssystem til at udføre en funktion”.*

*Ved juridisk person forstås, ”en enhed, der har status som juridisk person i henhold til den lovgivning, der finder anvendelse, med undtagelse af stater eller offentlige organer, der udøver deres statsmyndighed, eller offentlige internationale organisationer”.*

*Ved uretmæssig forstås, ”adfærd som omhandlet i dette direktiv, herunder adgang, indgreb eller opfangning, som ejeren eller en anden rettighedsindehaver af systemet eller en del af det ikke har givet tilladelse til, eller som ikke er tilladt i henhold til national lovgivning”.*

Der består en vis cirkularitet i definitionerne af informationssystem og edb-data. Informationssystem beskrives ud fra at det behandler EDB-data og EDB-data beskrives som noget der behandles i et informationssystem. Helena Lybæk Guðmundsdóttir har fremlagt i sin p.hd., at det er uklarheder i definitionen af de forskellige IT-begreber, der kan være en af årsagerne til, at bestemmelser om hacking ikke har været særligt anvendt, trods en betydelig stigning i antallet af cyberangreb<sup>151</sup>.

Begrebet *uretmæssig* minder til dels om *uberettiget*, men hvor *uretmæssig* mere er møntet på om brugeren havde en reel ret til at tilgå systemet, er det danske begreb *uberettiget*, som tidligere beskrevet, noget bredere end en tilladelse til at tilgå systemet. I henhold til dansk ret kan en adgang nemlig godt være strafbar, selvom brugeren havde en legitim adgang, praksis er imidlertid ganske tilbageholdende i disse situationer, se herom kap. 3, afsnit 3.2.

Direktivet definerer *uretsmæssig* dels som det tilfælde hvor ejeren ikke har givet tilladelse, dels som en henvisning til national ret. Direktivets formål beskrives i præambelens afsnit 7 og 8 som bl.a. en tilnærmelse af stater definitioner af begreber vedrørende ulovlig adgang til informationssystemer. Det forekommer i strid hermed, at direktivet ved sin definition af *uretsmæssig* til dels henviser tilbage til national ret. De nationale domstole kan således frit udvikle deres egne definitioner af begrebet. Der er således ikke med direktivet sat nogen særlig begrænsning på de nationale hackingbestemmelser vedrørende kravet om *uretsmæssig*. Cybercrime konventionen<sup>152</sup> og rammeafgåelsen<sup>153</sup>, har den samme definition af begrebet. Det er efter det anførte svært at se, at direktivet på dette punkt bidrager til en fælles definition af begrebet *uretsmæssig*.

---

<sup>151</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 18 ff.

<sup>152</sup> Explanatory report, s. 8.

<sup>153</sup> Artikel 1, litra d.

### 1.3. De ulovlige handlinger

Direktivet kriminaliserer overordnet 5 forskellige handlinger; *adgang til informationssystemer, indgreb i informationssystemer, indgreb i data, opfangning og videregivelse/anvendelse af værktøjer*. I de følgende vil *ulovlig adgang til informationssystemer* og *ulovlig opfangning* behandles, da de to øvrige områder ikke har en relation til hacking.

#### 1.3.1. Ulovlig adgang til informationssystemer

Artikel 3 forpligter medlemsstaterne til at træffe *”de nødvendige foranstaltninger til at sikre, at det er strafbart forsætligt at skaffe sig uretmæssig adgang til et informationssystem eller en del heraf, når den strafbare handling er begået ved brud på en sikkerhedsforanstaltning, i det mindste i grovere tilfælde.”*

Artiklen svarer til dels til artikel 2 i rammeafgårelsen og artikel 2 i Cybercrime konventionen. Den største forskel ligger imidlertid ved, at der i direktivet stilles krav om, at den strafbare handling skal være begået ved brud på en sikkerhedsforanstaltning.

I en rapport fra september 2017, vurderede Europa-Kommissionen hvorvidt unionens medlemsstater havde implementeret direktivets bestemmelser. Kommissionen vurderede, at følgende medlemsstater havde implementeret artiklen: AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE og SK. I de resterende medlemsstater, var der ikke i de nationale bestemmelser fastsat, at handlingen var begået for at få adgang til hele eller kun en del af informationssystemet<sup>154</sup>.

Ligeledes vurderede Kommissionen, at anvendelsesområdet i en række medlemsstater (BE, BG, FR, HR, LU, MT, PT, RO, SI og UK), var bredere end direktivet, da der ikke var indlagt et krav om omgåelse af en sikkerhedsforanstaltning i disse bestemmelser<sup>155</sup>. Hvilket er det samme som kendes i dansk ret.

I § 263's adgangsbegreb ligger der ikke et krav om, at en sikkerhedsforanstaltning skal brydes, hvilket kan undres, da det er en naturlig del af hacking at bryde en sikkerhedsforanstaltning.

I 1985-betænkning var Straffelovrådet opmærksomme på, at al data er beskyttet af en eller anden form for sikkerhedsforanstaltning. Denne kan enten være fysisk, i form af at aflåse rum som dataanlæggene befinder sig i, eller digitale, f.eks. i form af adgangskoder<sup>156</sup>. På samme tid som Straffelovrådet var opmærksomme på sikkerhedsforanstaltningernes relevans, var de også opmærksomme på, at foranstaltningerne ikke altid er effektive, herom udtaltes:

*”Værdien af sikringer afhænger naturligvis af, i hvilket omfang de fungerer i praksis. F.eks. er initialidentificering ikke meget værd, hvis en terminal efterlades åbnet i frokostpausen, og passwords er ikke meget værd, hvis andre er bekendt med dem. Dertil kommer, at i stort set alle systemer vil programmører, der kender systemerne, kunne læse alle aktuelle initialer, passwords o.l.”*<sup>157</sup>

---

<sup>154</sup> Rapport fra Kommissionen til Europa-Parlamentet og Rådet COM(2017) 474, s. 7.

<sup>155</sup> Rapport fra Kommissionen til Europa-Parlamentet og Rådet COM(2017) 474, s. 7.

<sup>156</sup> Betænkning nr. 1032/1985, s. 12 ff.

<sup>157</sup> Betænkning nr. 1032/1985, s. 13.

Straffelovrådet ønskede således ikke at tilføje et krav om et brud på en sikkerhedsforanstaltning, af frygt for at visse tilfælde i så fald vil henstå som straffri, f.eks. hvor en person glemmer at logge ud. Imidlertid kan et modsat argument gøres gældende, netop at bestemmelsen får et for bredt anvendelsesområde, når der ikke stilles krav om et brud på en sikkerhedsforanstaltning.

Selv om der ikke i § 263, stk. 1 er indlagt et krav om brud på en sikkerhedsforanstaltning, indgår det i en eller anden udstrækning i dommerens vurdering af, hvorvidt adgangen har været uberettiget. I sager om hacking baserer dommerens vurdering sig ofte på udtalelser fra forurettede og sagkyndige vidner om, hvor sofistikeret og effektiv sikkerhedsforanstaltningen har været, samt hvor avanceret gerningsmandens metoder har været. Denne vurdering tager først og fremmest sigte på at udskille de tilfælde, hvor en gerningsperson har opnået adgang, men hvor vedkommende er uvidende herom<sup>158</sup>.

Som behandlet i kap. 3, afsnit 3.5 har Straffelovrådet imidlertid åbnet op for at anvende et kriterie, der lægger sig op ad et krav om brud på en sikkerhedsforanstaltning, da Straffelovrådet mener, at det bør have en betydning, hvorvidt de tilgængelige data er offentlige eller ikke-offentlige.

Justitsministeriet har vurderet, at dansk ret er i overensstemmelse med artikel 3, henset til tre forhold<sup>159</sup>.

For det første, da § 263, stk. 1 straffer den uberettigede adgang til en andens oplysninger, der er bestemt til at blive brugt i et informationssystem.

For det andet, da det efter § 301a er strafbart uretmæssigt at skaffe eller videregive koder eller andre adgangsmidler til informationssystemer.

For det tredje, at det efter § 279a er strafbart, hvis en person, for at skaffe sig eller andre en uberettiget vinding, har skaffet sig adgang til et informationssystem og retsstridigt foretaget ændringer, tilføjelser eller sletning af oplysninger eller programmer til elektronisk behandling.

Som tidligere benævnt, er der tale om et minimumsdirektiv, hvorfor medlemsstaterne kan lovgive bredere end det af direktivet fremsatte. Vi stiller os enige i Justitsministeriets betragtning om, at dansk ret er i overensstemmelse med direktivet. Dansk ret er dog noget bredere end direktivet, da der ikke er et krav om brud på en sikkerhedsforanstaltning, og at vi i 263a fremrykker fuldbyrdelsestidspunktet. Ifølge Det af Justitsministeriet anførte om § 279a undrer det lidt, at det er henført som argument under art. 3, da den nærmere bør henføres til art. 5.

### 1.3.2. Ulovlig opfangning

Artikel 6 forpligter medlemsstaterne til at træffe de *”nødvendige foranstaltninger til at sikre, at det er strafbart forsætligt og uretmæssigt ved hjælp af tekniske hjælpemidler at opfange ikke-offentlige overføringer af edb-data til, fra eller inden for et informationssystem, herunder elektromagnetisk udsending fra et informationssystem, der indeholder disse edb-data, i det mindste i grovere tilfælde.”*

Kommissionen vurderede i 2017, at følgende medlemsstater havde implementeret artiklen fuldt ud: CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK og UK (Gibraltar). I forhold til delen om aflytning af EDB-data, havde AT og BG begrænset delen til meddelelser, EE til observation af en person og FR og HU til korrespondance.

---

<sup>158</sup> Wachter Lentz – *Hacking og det digitale privatliv*, s. 149.

<sup>159</sup> Justitsministeriets notat om tilvalg af Cybercrime-direktivet, s. 4.

Desuden har flere lande ikke medtaget aflytning af elektromagnetisk stråling (BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI og UK (undtagen Gibraltar). Visse lande kræver særlig hensigt (AT, EL HU) eller specifikke supplerende handlinger (BG og HU)<sup>160</sup>.

Der findes ikke i dansk ret en bestemmelse som direkte kriminaliserer ulovlig opfangning, men i bund og grund er ulovlig opfangning hacking, bare hvor gerningsmandens mål ikke er data som ligger tilgængeligt på systemet nu, men derimod indkomne informationer.

Der er intet i § 263, stk. 1's ordlyd, forarbejder eller øvrig litteratur der udelukker at § 263, stk. 1 ikke finder anvendelse i tilfælde hvor måldata'ene ikke er tilgængelige i systemet ved selve indtrængningen, men først kommer gerningsmanden i hænde ved en overførsel.

Dansk ret er derfor umiddelbart i overensstemmelse med artikel 6, hvilket understøttes af Justitsministeriets notat herom<sup>161</sup>.

## 2. Den svenske lovgivning

Den danske og svenske regulering minder på mange områder om hinanden. I relation til hacking, er der imidlertid den forskel, at Sverige har implementeret direktivet. I de følgende afsnit, vil vi analysere den svenske retsstilling, særligt i relation til beskyttelsesobjektet og uberettiget adgang, og sammenligne denne med den danske regulering.

### 2.1. Den svenske hacking bestemmelse

Brotsbalken kap. 4, 9c § blev senest ændret ved Lag (2014:302), der bygger på prop. 2013/14:92, og lyder således:

*"Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.*

*2 st. Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömning av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art."*

9c § er indplaceret i kapitel 4, der har overskriften *"om brott mot frihet och frid"*. Bestemmelsen er således lig den danske, indplaceret i et kapitel der omhandler den personlige integritet.

---

<sup>160</sup> Rapport fra Kommissionen til Europa-Parlamentet og Rådet COM(2017) 474, s. 7.

<sup>161</sup> Justitsministeriets notat om tilvalg af Cybercrime direktivet, s. 6.

Som eksempler på områder, hvor bestemmelsen finder anvendelse er hacking, spredning af virus, DOS/DDOS-angreb blevet benævnt<sup>162</sup>.

Ligesom i den danske lovgivning, er der ikke et krav i den svenske om, at en form for sikkerhedsforanstaltning skal brydes, der er ikke engang krav om, at systemet der åbnes, er beskyttet. Det er således også ulovligt at tilgå oplysninger i et åbent system. Der er imidlertid krav om, at en sådan adgang skal kunne karakteriseres som værende *ulovlig*<sup>163</sup>. Så ligesom i den danske lovgivning er det altså ikke enhver adgang, der er ulovlig.

En person som har en lovlig adgang til et system, men anvender denne på en retsstridig måde, f.eks. ved at tilgå oplysninger der ikke har relevans for vedkommendes foreliggende arbejdsopgaver, vil i lighed med dansk ret kunne straffes efter kap. 4, 9c § BrB<sup>164</sup>.

Det er direkte udtalt i forarbejderne til den seneste større revision af kap. 4, 9c § BrB, at den svenske bestemmelse er i overensstemmelse med direktivet<sup>165</sup>. Hvilket understøttes af, at Sverige er fremhævet af Kommissionen som et af de lande, der fuldt ud har implementeret art. 3<sup>166</sup>.

For at komme den svenske regulering nærmere, er det nødvendigt at analysere på den svenske retspraksis, derfor har vi udvalgt to afgørelser, hvilke vil blive analyseret i de to følgende afsnit.

## 2.2. RH 2015:15 – Datasystemer

*RH 2015:15* er afsagt af Svea Hovrätt. I sagen havde en medarbejder T installeret programmet *Google Talk* på sin arbejds-PC. Medarbejderen havde ifølge medarbejderhåndbogen ikke ret til at installere uautoriserede programmer på PC'en, hvorfor spørgsmålet blev rejst, om T herved havde *infört en uppgift i register (indført information i et register)*, hvilket er strafbart som hacking efter kap. 4, 9c § BrB.

Retten udtalte, at Google Talk udgør information, som er omfattet af bestemmelsens ordlyd, så spørgsmålet herefter var, om denne information var blevet indført i et register.

Herom udtaltes, at det fremgår af rammeafgørelsen af 2005, at formålet med kriminaliseringen er, at straffe ulovlig indtrængning i informationssystemer. Desuden havde Högsta domstolen i *NJA 2014 p. 221* udtalt, at formålet med den svenske lov er generelt at beskytte data mod uautoriserede handlinger, uanset om handlingen indebærer en krænkelse af privatlivet eller ej.

I den svenske lovgivning skal *register* forstås som *uppgifter som är strukturerade på visst sätt*<sup>167</sup> (*information der er struktureret på en bestemt måde*), men yderligere fortolkning af begrebet fandtes ikke. Anklageren argumenterede ud fra dette for, at handlingen var omfattet af bestemmelsen, da Google Talks havde påvirket Windows Stifinder og Explorer.

Retten fandt, at en PC's fil og register system bliver påvirket, når et program er installeret på en computer. Imidlertid ville det være betænkeligt at anvende en så bred fortolkning af begrebet *register*, at alle ændringer

---

<sup>162</sup> Kommentaren til § 9c på <https://lagen.nu/1962:700>

<sup>163</sup> <https://lagen.nu/1962:700>, kommentar til kap. 4, 9 c §.

<sup>164</sup> <https://lagen.nu/1962:700>, kommentar til kap. 4, 9 c §.

<sup>165</sup> Prop 2013/14:92, s. 1.

<sup>166</sup> Rapport fra Kommissionen til Europa-Parlamentet og Rådet COM(2017) 474, s. 7.

<sup>167</sup> Prop 2006/07:66 s. 18.

i systemet er omfattet. Kap. 4, 9 c § beskytter lagret data, og T's handling var kun at installere et program, der påvirkede de programmer, der får computeren til at fungere, hvilket ikke konstituerer, at der er *infört en uppgift i register*. Retten bemærkede videre, at hvorvidt en sådan handling er imod interne regler i en virksomhed, er et helt andet spørgsmål, og har ikke betydning for hvorvidt en handling er i strid med kap. 4, 9c § BrB.

T blev herefter frifundet.

I sagen gik retten altså ind og vurderede, at selvom ordlyden umiddelbart ikke differentierede mellem forskellige registre, ville det være for betænkeligt at indføre en så bred fortolkning, at en situation som den ovenstående ville være omfattet af kap. 4, 9c § BrB.

Som redegjort for i kap. 3, afsnit 2 er der umiddelbart en sammenlignelig retsstilling i forhold til betingelsen om, at der i § 263, stk. 1 skal være tale om *"Datasystem eller data, som er bestemt til at bruges i et datasystem"*. I dansk ret lader det til, at § 263, stk. 1 ikke omfatter alle former for oplysninger, derimod skal der være tale om oplysninger, som har en vis beskyttelsesværdi, dog er det svært at kunne udtale noget konkret om, hvilke data der er beskyttet.

Noget lignende kan læses ud fra *RH 2015:15*, netop da retten lægger vægt på, at Google Talks kun medfører ændringer i programmer, som anvendes af systemet til at få det til at fungere, og at Google Talks reelt ikke influerer på disse programmers virke.

Umiddelbart består der en lighed her, men vi mangler imidlertid i dansk ret, at få en afgørelse der klart statuerer, at ikke alle data er beskyttelsesværdige, men at der derimod skal foretages en vurdering.

Svea Högretten lægger selv vægt på rammeafgørelsen af 2005 i forbindelse med sin afgørelse, og foruden det af retten fremførte, kan yderligere nævnes, at rammeafgørelsen netop selv opfordrer medlemsstaterne til at udvise varsomhed med at give lovgivningen et for bredt anvendelsesområde<sup>168</sup>. Dette understøtter netop, at *RH 2015:15* er i overensstemmelse med rammeafgørelsen af 2005. Såfremt Danmark også opfylder rammeafgørelsen, hvilket må antages at være tilfældet, da Danmark er bundet af den, bør der foreligge en lignende retstilstand i Danmark.

Selvom at *RH 2015:15* er afsagt før Sveriges implementering af Cybercrime direktivet, er der intet som taler for, at denne ville medføre en ændring i den svenske praksis. For det første da direktivets præambler klart tegner et billede af, at det er større angreb, som dette søger at kriminalisere, og for det andet, da præambel 11 netop nævner, at straf kan udelades i mindre grove tilfælde. For det tredje, da forarbejderne har udtalt, at den svenske lovgivning (bortset fra strafmaksimum), er i overensstemmelse med direktivet<sup>169</sup>. Der er således intet holdepunkt for, at sagen ville have faldet anderledes ud i dag.

---

<sup>168</sup> Rammeafgørelse 2005/222/RIA, præmis 13.

<sup>169</sup> Prop. 2013/14:92, s. 30.

### 2.3. NJA 2014 s. 221 – Ulovlig adgang

*NJA 2014 s. 221* er afsagt af Högsta domstolen. I sagen havde en politimand T foretaget flere søgninger om sig selv i politiets database, for at opnå indsigt i oplysninger som politiet havde gemt om ham. T havde, som en del af sit arbejde adgang til politiets interne system, hvor det er muligt at slå en person op, og herigennem opnå indsigt i både offentlige og fortrolige oplysninger. T foretog 3 søgninger, en angående sine pas-oplysninger, en angående sin ejendom og en om hvorvidt han var under mistanke for nogen forbrydelser, hvoraf det fremgik, at T var mistænkt for flere overtrædelser.

T Forsvarede sig med, at de to første søgninger angik enten offentligt tilgængelige oplysninger, eller oplysninger T kunne have skaffet på anden lovlig vis, T fandt det bare nemmere at anvende politiets system. Angående søgningen i det kriminelle register, var dette for at rense sit navn over for nogen af sine studerende, der spurgte T, om han var under efterforskning for nogen strafferetlige overtrædelser. Formålet med søgning var således, at kunne vedligeholde sin autoritet over for sine studerende.

Den svenske byret frifandt T for overtrædelse af kap. 4, 9c § BrB i relation opslagene i pas- og ejendomsregistret, da oplysningerne i disse registre var tilgængelige for T på anden vis. Derimod blev T straffet for opslaget i kriminalregistret.

Ved appeldomstolen blev T dømt for overtrædelse af kap. 4, 9c § BrB for alle tre opslag. Domstolen lagde vægt på, at selvom T havde adgang til visse af oplysningerne, var T ikke berettiget til at foretage søgningerne. Domstolen udtalte yderligere, at det strafbare element i 9 C § BrB ikke afhang af hvorvidt oplysningerne var beskyttelsesværdige, men derimod om selve indtrængningen i systemet var berettiget eller ej.

Högsta domstolen tiltrådte Hovrättens afgørelse. Högsta domstolen lagde til grund, at bestemmelsens formål var at beskytte data mod uautoriseret adgang, uanset om de tilgåede data indebærer en fredskrænkelse<sup>170</sup>. Yderligere lagde retten til grund, at en handling er ulovlig, såfremt den er udført uden samtykke fra den person, som har ret til at bestemme over dataene, og at handlingen savner hjemmel i lovgivningen. Det er ikke et krav for en overtrædelse, at handlingen er foretaget med et bestemt formål. Det er derimod selve indtrængningen, der er strafbar<sup>171</sup>.

Det handler således ikke om, hvilke oplysninger der de facto er tilgået, men blot om der er tale om en ulovlig adgang.

Tilgangen er meget sammenlignelig med den, der findes i de danske forarbejder til § 263, stk. 1, men som tidligere redegjort viser dansk praksis, at der lægges vægt på, hvilke oplysninger der faktisk tilgås.

Sammenlignes afgørelsen med *U.1996.979 Ø*, er det svært at finde et fælles ståsted i den danske og svenske lovgivning. I *U.1996.979 Ø* skaffede gerningsmanden sig adgang til oplysninger der angik andre, og det var fuldstændig ubestridt, at denne adgang ikke havde nogen relation til gerningsmandens arbejde. Landsretten valgte imidlertid at frifinde gerningsmanden, netop da adgangen fandtes at være berettiget. I *NJA 2014 s. 221* skaffede gerningsmanden sig adgang til oplysninger som angik ham selv, og igen var faktum det samme, nemlig at gerningsmanden havde en berettiget adgang til systemet, men at denne adgang blev anvendt uberettiget. Imidlertid fandt Högsta domstolen, at dette var en overtrædelse af kap. 4, 9 c § BrB, og ikke bare

---

<sup>170</sup> Præmis 4.

<sup>171</sup> Præmis 6.

for de oplysninger som gerningsmanden med rette kunne forvente var unddraget for offentligheden, men også de oplysninger som gerningsmanden kunne have skaffet sig ganske nemt og lovligt.

Sammenlignes der med *U.2017.3544Ø*, er dommene sammenlignelige i den forstand, at begge angik adgang til samfundskritiske systemer, og at gerningspersonen fandtes at have overtrådt det respektive lands hackingbestemmelse. Der hvor afgørelserne imidlertid divergerer er, at i den danske afgørelse var der tale om systemer, som gerningsmanden generelt ikke havde en berettiget adgang til, og de tilgæede data omhandlede andre end gerningsmanden.

Den største forskel mellem domstolene bunder umiddelbart ud i, hvordan de forstår begreberne *uberettiget adgang* og *olovligen tilgang*.

Sammenlignes de danske domme om medarbejdere med *NJA 2014, s. 221*, kan det udledes, at de danske domstole lægger særlig vægt på om medarbejderen har en autoriseret adgang til at tilgå datasystemerne, mens dommerne i svensk ret har en snævrere tilgang til deres krav om "olovligen tilgang". I havde i *NJA 2014 s. 221* en autoriseret adgang til datasystemet, men blev alligevel idømt straf. Kom en sag med samme fakta for de danske domstole, ville dommen formentlig have endt ud med en frifindelse.

Uagtet Danmark ikke er bundet af direktivet, er det ovenfor anførte egnet til at illustrere den forskydning i de nationale domstoles forståelse af uberettiget, og hvorfor det er problematisk, når direktivet overlader definitionen af *uretsmæssig* til national ret.

Dette er særdeles illustrativt for hele problemet omkring lovgivning imod IT-kriminalitet, netop at lovgivningen generelt set virker vag, hvilket kan medføre, at domstole kan nå til vidt forskellige afgørelser, på trods af at lovgivningen bunder ud i samme regulering.

I sin ph.d. fremhæver Helene Lybæk, at en af de største vanskeligheder ved kriminaliseringen af IT-kriminalitet er, at vage juridiske begreber blandes med vage IT-begreber. Dette skaber en farlig cocktail, der medfører en betydelige usikkerhed for retsanvendelsen, netop da der ikke bare er en juridisk tvivl (hvilket jo er meget normalt, da domstolene ikke skal være alt for bundet), men der også er en tvivl om selve rækkevidden af bestemmelsernes begreber<sup>172</sup>. Det lader til, at den danske og svenske lovgivning er eksempler på, hvordan ellers ganske ens bestemmelser kan fortolkes vidt forskelligt.

Det skal dog bemærkes, at den svenske afgørelse er fra 2015, hvorimod *U.1996.979Ø* er fra 1996. Den danske afgørelse er således kommet ud før rammeafgørelsen, men det er dog tvivlsomt om rammeafgørelsen ville have medført et anderledes udfald i dommen. Der synes i hvert fald hverken at være et ståsted i forarbejder, litteratur eller praksis der peger imod, at § 263, stk. 1 har undergået nogen særlig ændring efter rammeafgørelsen.

Derimod kan der føres et argument for, at den svenske afgørelse i dag ville falde anderledes ud. Efter afsigelsen af *NJA 2014 s. 221* har Sverige implementeret Cybercrime direktivet<sup>173</sup>, hvori der er sket en ændring ift. Præmis 13 i rammeafgørelsen. Cybercrime direktivets præmis 18 angår nemlig også personer der anvender sin berettigede adgang på en uberettiget måde. Præmis 18 lader til at skærpe den mere tilbageholdne retstilling, der blev fremsat i rammeafgørelsens præmis 13, netop ved at gå væk fra at omtale

---

<sup>172</sup> Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, s. 18.

<sup>173</sup> Cybercrime direktivet blev implementeret i svensk ret ved Lag (2014:302).

en *tilbageholdenhed* med at straffe for autoriserede adgange. Derimod nævnes det blot, at "*der bør i den nationale ret tages passende hensyn til sådanne omstændigheder i forbindelse med en straffesag*". Såfremt en lignende sag blev fremført for Högsta domstolen i dag, kunne der føres et argument for, at sagen kunne falde anderledes ud, såfremt domstolen anvender Cybercrime direktivet i sin fortolkning af kap. 4, 9 c § BrB, hvilket ville føre den svenske retsstilling tættere på den danske.

## 2.4. Sammenfatning

Dansk og svensk ret bygger begge grundlæggende på rammeafgørelse 2005/222/RIA, Sverige har imidlertid implementeret Cybercrime direktivet, der dog grundlæggende bygger på rammeafgørelsen. Herom kan det imidlertid bemærkes, at Justitsministeriet vurderede, at Danmark overholder Cybercrime direktivet, og at den svenske lovgivning ikke har gennemgået en materiel ændring efter direktivet (der er kun tilføjet en skærpet straf i stk. 2<sup>174</sup>).

Der er både ligheder og uligheder mellem den danske og svenske regulering. Helt overordnet har både Danmark og Sverige valgt at kriminalisere hacking ved at tilføje en ny bestemmelse til landenes respektive straffelov. Dog virker den svenske bestemmelse til at omfatte flere delikter end den danske, men dette skyldes umiddelbart blot, at hvor Sverige har valgt at implementere så meget af rammeafgørelsen/direktivet i en bestemmelse, er visse delikter omfattet af andre bestemmelser i dansk ret, f.eks. § 293, stk. 2 om DDOS angreb.

I forhold til forståelsen af de to centrale dele af bestemmelse, i form af hvilke data der er beskyttet, og hvordan ulovlig/uberettiget adgang skal forstås, ses der både ligheder og forskelle.

I forhold til spørgsmålet om hvilke data der er beskyttet, ses der et vist sammenfald mellem svensk praksis og danske forarbejder/litteratur. Både dansk og svensk ret lader til at ville udskille visse data som ikke beskyttelsesværdige. I dansk ret mangler der imidlertid praksis herom. Efter *RH2015:15* har svensk retspraksis imidlertid nærmet sig en noget mere klar retsstilling, da retten direkte udtalte, at de programmer som blot anvendes af systemet, og ikke indeholder nogen særlige oplysninger, ikke bør nyde beskyttelse efter kap. 4, 9 c § BrB, i en sag som den foreliggende. En sådan praksis må klart siges at være i overensstemmelse med rammeafgørelsen og Cybercrime direktivet.

I forhold til *ulovlig/uberettiget adgang* lader der til at være ganske store uoverensstemmelser mellem dansk og svensk retspraksis. Svensk retspraksis lader til at have en markant mere restriktiv forståelse af hvad *ulovlig adgang* er. Der lægges umiddelbart ikke lige så meget vægt på, at adgangen har været autoriseret. En retsstilling der kan undre lidt, da det er fremført i rammeafgørelsen af 2005's præambel 13, at medlemsstaterne skal søge at undgå en overkriminalisering, herunder i tilfælde hvor der er tale om en autoriseret adgang. Det kan altså virke som en overkriminalisering, at straffe en person for hacking, når denne, med autorisation, tilgår offentlige oplysninger om sig selv. På samme tid kan det virke som en underkriminalisering ikke at straffe en person der tilgår ikke-offentlige oplysninger om andre. Uanset hvordan retsstillingen bør være, kan det blot her konstateres, at der eksisterer en ganske betydelig forskel mellem dansk og svensk ret.

---

<sup>174</sup> Se herom Prop. 2013/14:92.

## Kapitel 5

### 1. Retspolitisk vurdering

Meget er ændret i verden siden indførelsen af § 263, stk. 1 i 1985, Berlinmuren faldt, Danmark vandt EM og internettet former i dag vor hverdag. Internet of Things er fuldstændig eksploderet. I dag er internettet koblet op til alt fra ure til samfundskritiske systemer. Dette har ændret den måde vi anvender systemer. Hvor datasystemer førhen var simple systemer, der sjældent var tilsluttet terminaler, og ikke indeholdte et væld af oplysninger, indeholder nutidens datasystemer et væld af oplysninger, og er koblet op til internettet.

Strafferettens fornemmeste opgave er at fastsætte autoritative adfærdsnormer. Straffeloven kan ses som et katalog over handlinger og undladelser, som lovgiver anser som værende uønskede i samfundet. Den strafferetlige regulering bør altid afspejle sig i den verden vi lever i<sup>175</sup>, og et af strafferettens idealer er at udfærdige straffebestemmelser på baggrund af borgerens adfærd og de sociale normer i samfundet<sup>176</sup>.

Der kan i dagens samfund ikke være nogen i tvivl om, at decideret hacking er ulovligt. Der hvor den strafferetlige lovgivningsopgave bliver udfordret, er derimod i de tilfælde hvor almindelige borgere har deres daglige gøren og laden med datasystemer og internettet. Internettet, og den stadigt stigende udbredelse af datasystemer, har medført nogle nye og anderledes handlemønstre end vi kender fra den fysiske verden. Derfor ses der forskelle mellem de kriminaliserede handlinger og de sociale normer og kutyper, der har udviklet sig omkring brugen af datasystemer.

Den nuværende affattelse af § 263, stk. 1, byder både på fordele og ulemper.

Fordelen ved § 263, stk. 1 og dennes brede formulering er, at den kan omfatte stort set alle tilfælde af adgang til data/datasystemer, men samtidig giver mulighed for konkrete vurderinger. Denne konstruktion er hensigtsmæssig i en tid, hvor teknologien er i voldsom udvikling, og hvor vi som samfund er ved at danne os en mening om, hvad der er og ikke er tilladt i det digitale landskab.

Bestemmelsens upræcise begreber, er samtidig et af de største kritikpunkter, da de giver et væld af problemer i forhold til dens anvendelse.

For hvordan er det helt præcist, at vi skal forstå en *uberettiget adgang*? Hvis jeg f.eks. tilgår en hjemmeside, der sælger produkter i flere lande, vil jeg automatisk blive omdirigeret til den danske hjemmeside, med de tilhørende danske priser. Tilgår jeg nu hjemmesiden med en VPN, der er sat til Rusland, vil jeg kunne tilgå hjemmesiden med de tilhørende lavere russiske priser. Hjemmesiden jeg tilgår er åben for alle, men det er åbenlyst, at ejeren ikke ønsker, at jeg tilgår hjemmesiden igennem en VPN. Vil dette udgøre *uberettiget adgang*?

Et andet kritikpunkt er, at bestemmelsen er underlagt betinget offentlig påtale. Retspraksis bliver sparsom, da det typisk er virksomheder der rammes af angreb. Virksomheder føler sig ikke ligesom personer inkrimineret, og de ønsker ikke at eksponere sig selv ved at anmelde forholdet til politiet. Hvorfor mange sager aldrig når til domstolene.

---

<sup>175</sup> Vestergaard – *Strafferetlige sanktioner*, s. 5.

<sup>176</sup> Bo Langsted – *Strafferettens almindelige del*, s. 92.

Det er desuden problematisk, da det ikke er ligetil at afgøre, hvem der reelt er påtaleberettiget. Problemet er, at vi i dag giver vores oplysninger ud til både private og virksomheder, der så lagrer oplysningerne i deres systemer. Bliver oplysningerne hacket, kan det være svært at afgøre hvem der reelt er påtaleberettiget, og det kan være svært for den som oplysningerne angår, at anmelde sagen selv hvis vedkommende vurderes til at være påtaleberettiget.

Som eksempel herpå kan nævnes, at hvis Facebook bliver hacket, så er Facebook selvfølgelig påtaleberettiget, men hvis nu de hakede oplysninger angår dets brugere, bliver spørgsmålet, om brugerne i så fald også er påtaleberettigede. Selv hvis brugerne er påtaleberettiget, opstår det problem, at Facebook højst sandsynligt vil forsøge at skjule, at de er blevet hacket, for ikke at miste brugernes tillid. Selv hvis brugerne skulle være påtaleberettiget, vil de i så fald ikke have et tilstrækkeligt oplyst grundlag, til at kunne anmelde sagen. Denne konstruktion bidrager til, at hackere kan vedligeholde kadencen på hacking-området, da risikoen for at blive efterforsket er uforholdsmæssig lav.

Sættes påtalereglerne op imod datasystemer i 1985, gav det nok en vis mening at anvende betinget offentlig påtale, netop da datasystemer primært var forbehold offentlige institutioner, banker, o.lign. Men i dag hvor alle ejer mindst et datasystem, vores oplysninger er spredt ud, og at målet typisk er virksomheder, burde det nok overvejes at fjerne den betingede offentlige påtale.

Straffelovrådet overvejede i betænkning 1563/2017, at fjerne den betingede offentlige påtale. Set ud fra en juridisk synsvinkel fandt Straffelovrådet det anbefalelsesværdigt at fjerne den betingede påtale, men endte med ikke at anbefale det, henset til de økonomiske omkostninger der ville være forbundet hermed<sup>177</sup>.

Rammeafgørelsen<sup>178</sup> og Cybercrime direktivet<sup>179</sup>, indeholder begge henvisninger til at der bør være en bagatelgrænse. Forarbejderne og retspraksis til § 263, stk. 1 er alligevel tavse herom, hvorfor det er svært at sige noget herom. Men hvis der skal findes en bagatelgrænse, hvordan skal denne så fastlægges? Skal vi se bagatelgrænsen ud fra, den måde gerningspersonen tilgår datasystemet på, eller ud fra de data der opnås adgang til, eller evt. en samlet vurdering?

Skulle bagatelgrænsen findes igennem kravet om en *uberettiget adgang*, kunne grænsen tænkes at bunde i parternes indbyrdes relation, sociale normer eller handlingens karakter. Der ses hverken i praksis eller forarbejder nogle pejlemærker til fastlæggelsen af en bagatelgrænse. Henset til eksisterende praksis, se hertil U.2017.246V og U.2015.345Ø, er grænsen dog nok sat relativt lavt. Der bør dog, henset til de bagvedliggende retsgrundlag navnlig Cybercrime konventionen og rammeafgørelsen, være en bagatelgrænse.

Bagatelgrænsen kan også tænkes at skulle søges i hvilke *data* eller *datasystemer*, der er opnået adgang til. Der findes ikke dansk retspraksis der statuerer en bagatelgrænse baseret på typen af data eller datasystem, men i svensk ret er det helt klart, at der eksisterer en mindstegrænse henset til RH 2015:15. Såfremt bestemmelsen ikke skal overkriminalisere, er det, som også anført af den svenske Högsta Domstolen, formålstjenstligt ikke at kriminalisere enhver adgang til data eller datasystemer, da ikke alle data eller datasystemer er beskyttelsesverdige. En bagatelgrænse her ville ej heller medføre, at gerninger som ellers

---

<sup>177</sup> Betænkning nr. 1563/2017, s. 170.

<sup>178</sup> Præmis 13.

<sup>179</sup> Artikel 3 og Forslag Cybercrime Direktivet KOM(2010/0273 (COD), s. 8.

bør straffes undgår sanktion. For såfremt en gerningsperson havde til hensigt at få adgang til beskyttelsesværdige data, men disse ikke ligger på systemet, vil gerningspersonen kunne straffes for forsøg.

Sagernes kompleksitet gør imidlertid, at det er forsimplet, at statuere at bagatelgrænsen igennem et af begreberne, da det i sidste ende nok bør søges igennem en helhedsvurdering af sagens omstændigheder. Ovenstående skal derfor blot ses som eksempler på momenter, der kunne inddrages i denne vurdering.

## 2. Konklusion

Projektet søgte at afklare anvendelsesområdet for § 263, stk. 1. For at afklare dennes grænser dissekerede og analyserede vi bestemmelsens enkelte begreber, og holdt bestemmelsen op mod legalitetsprincippet, EU-ret og svensk ret.

Om begrebet uberettiget kan siges, at dette er blevet indført som en konsekvens af bestemmelsens brede formulering, og dennes evne til at omfatte en stor mængde forhold. Tilfælde hvor gerningspersonen som fuldstændig udenforstående opnår adgang, og tilfælde hvor bemyndigede personer klart overskrider deres bemyndigelse, er som udgangspunkt uberettiget. I de andre tilfælde signalerer begrebet, at der skal foretages en rimelighedstest. Rimelighedstesten indebærer en konkret vurdering af det foreliggende tilfælde, hvor et væld af momenter kan inddrages f.eks. parternes relationer, samtykke, materiel atypicitet osv.

I relation til ovenstående står det klart, at der gælder en særlig modifikation i forhold til medarbejdere. Ved disse lader det til, at der skal mere til før de har overtrådt § 263, stk. 1. Denne modifikation gælder selvom, at den konkrete handling findes at foreligge uden for det forefaldende arbejde. Modifikationen kan forsvares ud fra to henseender. For det første, da de har en berettiget adgang som led i deres arbejde. For det andet, da det kan virke mere proportionelt at lade *straffen* være op til arbejdsgiveren, der kan sanktionere medarbejderen i overensstemmelse med de gældende regler på det arbejdsmarkedsretlige område.

Om begreberne *uberettiget* og *adgang*, er det gennem analysen blevet klart, at disse to begreber ikke kan adskilles, da det ikke giver mening at snakke om uberettiget, uden samtidigt at se på hvordan adgangen er opnået.

Ses der alligevel på begrebet *adgang* separat, er der ikke megen vejledning at hente, andet end at der skal være opnået forbindelse til systemets indhold. Ud fra Cybercrime konventionen og den tilhørende explanatory report kan yderligere udledes, at grænsen for adgang går et sted mellem den blotte tilsendelse af en e-mail og en hjemmesides placering af cookies på den besøgende computer. Der findes ikke dansk retspraksis, der problematiserer begrebet adgang.

§ 263, stk. 1 kan ikke antages at være i strid med legalitetsprincippet, hverken efter § 1 eller menneskerettighedskonventionens artikel 8. I dansk ret bliver bestemmelser ikke uanvendelige eller ugyldige, fordi deres ordlyd er bred eller begreber uklare. Derimod er det overlagt til dommeren at søge bestemmelsens anvendelsesområde afklaret igennem de almindelige fortolkningsprincipper. Legalitetsprincippet i art. 8, divergerer derimod fra det danske. Heri ligger nemlig krav om, at bestemmelsen skal være *tilgængelig* og *forudsigelig*. Umiddelbart er der intet som taler særligt for, at § 263, stk. 1 skulle være i strid hermed.

I relation til Cybercrime direktivet, har vi analyseret direktivets artikel 3 om ulovlig adgang til informationssystemer og artikel 6 om ulovlig opfangning. Artikel 3 var i 2017, ifølge Kommissionen, fuldt implementeret af 15 medlemsstater, delvist implementeret af 10 medlemsstater, og ikke implementeret af 2. Vi sammenholdt herefter artikel 6's anvendelsesområdet med de i straffeloven relevante bestemmelser. I forhold til art. 6 fandtes, at dansk ret kriminaliserer hacking noget bredere end direktivet fastsætter, men da der er tale om et minimumsdirektiv, er dansk ret, som også anført af Justitsministeriet, i overensstemmelse med direktivet. Da hacking, og cybercrime generelt, er meget internationale kriminalitetsformer, er det vigtigt at dansk ret overholder minimumskravene, selvom at Danmark ikke har implementeret direktivet. I forhold til artikel 6 fandtes, at dansk ret også overholder denne, da dennes anvendelsesområdet kan omfattes af § 263, stk. 1, dog fandtes dansk ret ikke at gå længere end artiklens anvendelsesområdet.

Vi sammenholdt § 263, stk. 1 med Brottsbalken kap. 4, 9c §, hvor der var særligt fokus på de to områder *beskyttelsesobjektet* og *uberettiget/ulovlig adgang*. I Svensk ret er retsstillingen angående *register* (data/datasystem) klarere end den danske. Som det fremgår af RH 2015:15 fortolkes *register* i svensk ret bredt. Dog ses der i dommen, at standard systemfiler ikke i det konkrete tilfælde omfattes af beskyttelsen. Der kan af dommen udledes, at der i svensk ret findes en bagatelgrænse, og som dommen antyder, sættes denne lavt. I dansk ret er retsstillingen på dette punkt endnu ikke klar.

For så vidt angår anvendelsen af begrebet ulovlig/uberettiget adgang, er den svenske tilgang til begrebet ret bredt, således at den adgang en medarbejder - der i øvrigt har autoriseret adgang – opnår til et system ikke nødvendigvis er berettiget. I dansk ret, lader det til at domstolene ser på om medarbejderen har autoriseret adgang, og derefter som udgangspunkt anser adgangen som berettiget.

Helt generelt kan det afslutningsvist konkluderes, at § 263, stk. 1 særligt er problematisk i to henseender. For det først da bestemmelsen er et forsøg på at kombinere jura og IT, hvilket begge er områder karakteriserede ved uklare og vage begreber. For det andet da der i det væsentligste mangler fortolkningsbidrag til bestemmelsen. Der findes ikke megen trykt praksis, litteraturen er enormt kortfattet og forarbejderne er sjældent særlig konkrete. Ovenstående gør netop, at selvom bestemmelsen har eksisteret siden 1985, og angår et enormt relevant område, vides der egentlig ikke meget om dens anvendelsesområde.

# Litteraturliste

## Betænkninger

Betænkning nr. 601/1971

Betænkning nr. 1032/1985

Betænkning nr. 1417/2002

Betænkning nr. 1494/2008

Betænkning nr. 1563/2017

## Svenske betænkninger

Prop. 2013/14:92

Prop. 2006/07:66

## Folketingstidende

Folketingstidende samling 1991-92, Tillæg A

Folketingstidende samling 1999-00, Tillæg A

Folketingstidende samling 2003-04, Tillæg A

Folketingstidende, samling 2018-19, Tillæg A

## Bøger

August Herman Ferdinand Carl Goos – *Den Danske strafferets specielle del 1*, 1895, Gyldendalske boghandels forlag

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

Gorm Toftegaard Nielsen, Thomas Elholm og Morten Niels Jakobsen – *Kommenteret straffelov Speciel del*, 11. omarbejdede udgave, 2017, Jurist- og Økonomforbundets forlag.

Jan Trzaskowski, Søren Sandfeld Jakobsen, Susanne Karstoft, Hanne Kirk, Lars Bo Langsted, Thomas Riis, Charlotte Bagger Tranberg og Helena Lybæk Guðmundsdóttir – *Internetretten*, 3. udgave, 2017, Ex Tuto Publishing

Jørn Vestergaard – *Strafferetlige sanktioner*, 1. udgave, 2012, Gjellerup

Knud Waaben & Lars Bo Langsted – *Strafferettens almindelige del*, 6. reviderede udgave, 2015, Karnov Group Denmark

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

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

Ole Spiermann – *Moderne folkeret*, 3. udgave, 2006, Jurist- og Økonomforbundets forlag

Sten Bønsing, Thomas Elholm, Søren Sandfeld Jakobsen og Lene Wachter Lentz – *I forskningens og formidlingens tjeneste – festskrift til professor Lars Bo Langsted*, 1. udgave, 2018, Ex Tuto Publishing

Trine Baumbach – *Strafferet og menneskeret*, 1. udgave, 2014, Karnov Group Denmark

Vagn Greve, Poul Dahl Jensen og Gorm Toftegaard Nielsen – *Kommenteret Straffelov almindelige del*, 10. omarbejdede udgave, 2013, Jurist- og Økonomforbundets forlag.

Vagn Greve – *EDB-strafferet*, 1984, Jurist- og Økonomforbundets forlag

#### **ph.d.**

Helena Lybæk Guðmundsdóttir – *Clarifying broad hacking statutes*, 2015, Aalborg Universitetsforlag

#### **Artikler**

Orin S. Kerr – *The Problem of Perspective in Internet Law*, 2003, Georgetown Law Journal, Vol 91.

U.1998B.270/3 – *Jørn Vestergaard og Flemming Balvig (red.): »Medlov . . .«. Retsvidenskabelige betragtninger*, Jurist- og Økonomforbundets Forlag 1998, 350 sider. Af Gorm Toftegaard Nielsen

Lene Wachter Lentz – *Hacking og det digitale privatliv*, Juristen nr. 4, 2018.

#### **Rapporter**

Center for Cybersikkerhed – *Trusselsvurdering – Cybertruslen mod Danmark*, Maj 2018.

Council of Europe – *Explanatory report to the Convention on Cybercrime*, European Treaty series – 185, 2001.

Council of Europe – *T-CY Guidance Note #2 Provisions of the Budapest Convention covering botnets*, 2013.

World Economic Forum – *The Global Risks Report 2019*

## **EU**

COM(2017) 474 – *Rapport fra Kommissionen til Europa-parlamentet og Rådet om vurdering af, i hvilket omfang medlemsstaterne har truffet de nødvendige foranstaltninger til at overholde direktiv 2013/40/EU om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/JHA*

KOM(2008) 448 – *Beretning fra Kommissionen til Rådet i henhold til artikel 12 i rådets rammeafgørelse af 24. februar 2005 om angreb på informationssystemer*

Forslag Cybercrime Direktivet KOM(2010/0273 (COD)

## **Pressemeddelelser**

Topdanmark – Pressemeddelelse nr. 20/2010 af 07/12/2010: "Topdanmark has been a victim of URL hacking"

## **Websites**

<https://politi.dk/rigspolitiet/nyhedsliste/politiet-slaar-ned-paa-ddosangreb/2019/01/28>

<https://lagen.nu/1962:700>

<https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>

<https://webfoundation.org/2019/03/web-birthday-30/>

## **Ugeskrift for Retsvæsen**

U.1969.56H

U.1987.216Ø

U.1988.372H

U.1989.688H

U.1991.85H

U.1992.16V

U.1995.405V

U.1996.979Ø

U.1997.634V

U.2000.1450Ø

U.2015.345Ø

U.2015.1525H

U.2015.3615Ø

U.2016.2666V

U.2017.247V

U.2017.3544Ø

U.2018.1787H

#### **Tidsskrift for Kriminalret**

TfK2017.1034

TfK2013.240

#### **Rättsfall Hovrätter**

RH 2015:15

#### **Nytt Juridiskt Arkiv**

NJA 2014 s. 221

#### **Utrykt**

Østre Landsrets ankedom af 7. marts 2017 – S-2696-16

#### **Menneskerettighedsdomstolen**

Wingrove v. the United Kingdom - app no. 17419/90 afgørelse af 25. november 1990

Schimanek v. Austria – app. No. 32307/96 afgørelse af 1. februar 2000

Kafkaris v. Cyprus – app.no. 21906/04, afgørelse af 12. februar 2008

#### **Notater**

Justitsministeriets notat om tilvalg af Cybercrime direktivet

Ordoptælling?×

Statistik:

|                       |         |
|-----------------------|---------|
| Sider                 | 63      |
| Ord                   | 25.203  |
| Tegn (uden mellemrum) | 142.881 |
| Tegn (med mellemrum)  | 167.573 |
| Afsnit                | 771     |
| Linjer                | 2.160   |

☒ Medtag tekstfelter, fodnoter og slutnoter

Luk