AALBORG UNIVERSITET

Retlige udfordringer ved efterforskning og tiltalerejsning i forhold til databedrageri

- En analyse af straffelovens § 279 a

Kandidatspeciale af Mette Bæk Sørensen og Sarah Maria October Thomsen

Vejleder: Hanne Hartoft

Afleveret: 18. maj 2019

Indholdsfortegnelse

Abstract

The subject of this thesis is to examine the legal challenges of investigation and prosecution regarding data fraud. This leads to a more thorough analysis of the boundaries between §§ 279a (data fraud) and 276 (theft), 279 (fraud), and 301(skimming) of the Danish Criminal Code.

Subsequently the thesis also investigates why § 799 (secret searches) of the Administration of Justice Act is applicable to grand theft, cf. § 286 (1) cf. § 276 and not aggravated data fraud, cf. § 286 (2) cf. § 279a.

In addition to this problem the thesis will look into whether secret searches have kept up with the technological development or whether the provision needs to be amended.

By examining the report no. 1032/1985 on data-crime it can be concluded that the boundaries between §§ 279 and 279a is to be determined by the level of human involvement in the course of criminal events.

On the basis of relevant case law it can furthermore be concluded that the boundaries between §§ 276 and 279a is now established when it comes to credit card fraud. Thus the preliminary theft of credit cards falls within § 276, and the subsequent usage of the credit cards falls within § 279a.

The boundaries between §§ 301 and 279a is relevant when the perpetrator obtains the credit card information. The problem is to determine whether § 301 is absorbed by § 279a, cf. 21 (attempted data fraud). Case law shows that the perpetrator is charged with both provisions.

By examining the purpose of secret searches cf. § 799 of the Administration of Justice Act it seems that there are no reasons why this measure should not apply to investigation of § 286(2), cf. § 279a of the Danish Criminal Code. However it seems that the reason why it does not apply is a result of legislators not wanting to expand the provision due to the measures serious infringement upon individual rights.

Finally it can be concluded that the problem with secret searches in regards to data fraud can be remedied by only letting § 799 cover physical secret searches. Secret searches on a communication platform should then be covered by § 791b (data-monitoring) instead of § 799.

This amendment would make the work of police investigation and the prosecution more consistent and streamlined.

Kapitel 1 - Indledning

I 1984 gjorde en person ved navn Viggo sig selv til genstand for stor medieomtale, fordi han påstod, at han flere gange havde "skaffet sig adgang til offentlige og private EDB-systemer"[1], ved hjælp af en computer[2]. Det viste sig senere, at Viggos påstande ikke var sandfærdige, men de gav anledning til en revurdering af, hvorvidt straffelovens gældende regler omfattede kriminelle forhold der blev begået ved hjælp af IT. Der var tale om en ny kriminalitetstype, der resulterede i, at Straffelovrådet afgav en betænkning i 1985 om datakrimnalitet[3]. På denne baggrund fremsatte Justitsministeren et lovforslag[4], der bl.a. indeholdt en bestemmelse om databedrageri i strfl. § 279 a, som blev vedtaget kort tid efter. Vedtagelsen af dette lovforslag var banebrydende, da der på daværende tidspunkt kun i enkelte stater i USA var specifik lovgivning vedrørende forbrydelser begået ved hjælp af IT. Danmark blev derved det første land i Europa, som indførte specielle straffebestemmelser om IT-kriminalitet[5].

Efterfølgende har det vist sig, at lovgiver har været meget fremadskuende på dette område, da IT-kriminalitet i de følgende årtier har været stødt stigende[6]. Dette skyldes den voldsomme udvikling som teknologien har undergået siden 80'erne, hvor de første hjemmecomputere, som vi kender dem i dag blev lanceret[7]. Således viser tal fra Rigspolitiets Statistikenhed, at antallet af anmeldelser om databedrageri er steget i perioden 2010-2018, hvor antallet af anmeldelser gik fra ca. 1.400 til 20.000[8]. Der er intet der tyder på, at IT-kriminalitet ikke også vil være en betydelig del af kriminalitetsbilledet i de kommende år. Dette skyldes, at der i forbindelse med politiets indsats mod bekæmpelse af IT-kriminalitet er en risiko for, at de kriminelle tilpasser

[1] Carlsen og Elmer, Juristen 1986, Datakriminalitet, s. 297
[2] Der er ikke en entydig definition af, hvad en computer er. Dette skyldes især den drastiske udvikling, som computere har undergået med hensyn til funktion og opbygning, siden deres oprindelse. Generelt adskiller computere sig fra andre maskiner ved, at der foretages elektronisk databehandling, jf. Greve, EDB-strafferet, 1986, s. 17. Computere kan optræde i mange forskellige former og have forskellige funktioner, jf. betænkning nr. 1417/2002, pkt. 2.2
[3] Betænkning nr. 1032/1985
[4] LFF 1985-04-24 nr. 221
[5] Carlsen og Elmer, Juristen 1986, Datakriminalitet, s. 297
[6] Kruize, Det Kriminalpræventive Råd, Internetkriminalitet, 2017. Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace, s. 6 og Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed, s. 1
[7] http://nyheder.tv2.dk/tech/2016-08-12-pcen-fylder-35-aar-var-taet-paa-ikke-at-lykkes, (tilgået d. 16/5-19)
[8] Se bilag 1 og 2

sig og udvikler nye metoder til at begå kriminalitet på internettet[9]. Behovet for at undersøge, hvilke udfordringer som indførelsen af strfl. § 279 a har medført, er derfor relevant.

Et område der har skabt vanskeligheder for anklagemyndigheden i forbindelse med tiltalerejsning, har været anvendelsesområdet for bestemmelsen om databedrageri, jf. strfl. § 279 a. Strfl. § 279 a blev i en årrække tillagt en indskrænkende fortolkning, hvilket har medført et stort mørketal i henhold til begåede databedrageriforhold[10]. Grundlaget for den indskrænkende fortolkning har primært været et udslag af udfordringer med hensyn til grænsedragningen mellem databedrageri, jf. strfl. § 279 a og tyveri efter strfl. § 276. Det er derfor interessant at undersøge, hvorfor der har været problemer med at afgrænse bestemmelserne over for hinanden, og hvorfor denne afgrænsning er relevant i forhold til IT-kriminalitet.

Udover problemstillingen omkring grænsedragningen fra de traditionelle berigelsesforbrydelser, har indførelsen af strfl. § 279 a også medført nogle udfordringer ved efterforskningen. Særligt er politiets mulighed for at foretage hemmelig ransagning ved databedrageri efter rpl. § 799 blevet fremhævet, som en efterforskningsmæssig udfordring. "Rigsadvokaten har over for justitsministeriet gjort opmærksom på, at mange kriminelle handlinger i stadig større udstrækning foretages digitalt, og at efterforskningen af disse handlinger derfor også foregår digitalt. Dette kan i praksis give anledning til problemer, da retsplejelovens bestemmelser om tvangsindgreb ikke fuldt ud tager højde for denne udvikling."[11] Det er derfor relevant at undersøge om der er behov for en tilpasning af rpl. § 799 i forhold til databedrageri.

På trods af, at bestemmelsen om databedrageri blev indført i 80'erne, og selv om den eksplosive teknologiske udvikling har gjort bestemmelsen særligt relevant, er den kun blevet behandlet overfladisk i den juridiske litteratur[12]. Dette har givet inspiration til at foretage en dybdegående analyse af visse problemstillinger omkring bestemmelsen.

---

[9] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 4

[10] "Det har vist sig, at anklagemyndigheden, navnlig frem til dommen U 2014.1688 V, anlagde en indskrænkende fortolkning af bestemmelsen, der i en årrække gjorde, at § 279 a ikke blev benyttet i det omfang, kriminalitetsbilledet rent faktisk tilsagde", jf. Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed, s. 1

[11] Lovudkast L105, alm. bem., pkt. 2.7.2.

[12] Røn, Databedrageri - stadig en overset bestemmelse?, 2018, s. 295

1.1 Problemformulering

Det overordnede tema for dette speciale er: Retlige udfordringer ved efterforskning og tiltalerejsning i forhold til databedrageri. Under dette emne vil vi foretage en undersøgelse af betydning af afgrænsningen mellem databedrageri (strfl. § 279 a) og straffelovens bestemmelser om bedrageri (strfl. § 279), tyveri (strfl. § 276) og skimming (strfl. § 301). Derudover vil det blive undersøgt om reglerne om hemmelig ransagning (rpl. § 799) er hensigtsmæssige i forhold til efterforskning af databedrageri i det virtuelle univers - det vil sige, hvor der sker retsstridig påvirkning af en computer frem for et menneske.

Dette vil primært blive behandlet inden for den type af databedrageri der omfatter uberettiget brug af betalingskort. I den forbindelse vil der blive lagt vægt på følgende problemstillinger:

- Anvendelsesområdet for strfl. § 279 a - hvordan adskiller databedrageri sig fra almindeligt bedrageri (strfl. § 279)?
- Hvilke udfordringer har afgrænsning mellem strfl. §§ 276 og 279 a medført i forbindelse med tiltalerejsning?
- Afgrænsningen mellem strfl. §§ 279 a og 301
- Hvorfor er der ikke hjemmel til hemmelig ransagning ved databedrageri af grov beskaffenhed - har indførelsen af strfl. § 279 a medført problemer i forbindelse med efterforskning ved, at kriminaliteten er rykket på internettet?
    - Samspillet mellem hemmelig ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning i forhold til databedrageri
    - Baggrunden for indførelsen af rpl. § 799 - hvorfor finder indgrebet anvendelse ved strfl. § 286, stk. 1, jf. § 276 men ikke ved strfl. § 286, stk. 2, jf. § 279 a eller strfl. § 301, stk. 2, jf. stk. 1?
    - Bør bestemmelsen bestemmelsen om hemmelig ransagning revideres?

1.2 Afgrænsning

I dette speciale bliver bestemmelsen om databedrageri, jf. strfl. § 279 a, beskrevet og analyseret i forhold til andre udvalgte berigelsesforbrydelser, herunder strfl. § 279 om bedrageri, § 276 om tyveri og § 301[13] om anskaffelse af betalingskortoplysninger mv.. Dommen U 2014.1688 V er i den forbindelse et vigtig fortolkningsbidrag til retstilstanden i forhold til afgrænsningen mellem strfl. §§ 279 a og 276, hvorfor denne dom vil blive analyseret dybdegående.

Straffelovens § 279 a afgrænses ofte også i forhold til § 278 om underslæb, § 280 om mandatsvig og § 283 om skyldnersvig, men vi har valgt ikke inddrage disse bestemmelser, da denne afgrænsning allerede er blevet behandlet dybdegående[14].

Formålet med afgrænsningen i forhold til strfl. §§ 279, 276 og 301 er at fastslå anvendelsesområdet for strfl. § 279 a, og derved fastslå i hvilke tilfælde bestemmelsen finder anvendelse.

På baggrund af afgrænsningen mellem strfl. §§ 276 og 279 a, vil der blive foretaget en analyse af, hvorfor der er hjemmel til hemmelig ransagning, jf. retsplejelovens § 799, ved groft tyveri, men ikke ved databedrageri eller skimming af grov beskaffenhed. Denne hjemmelsmæssige problematik er over for Justitsministeren blevet påtalt af Rigsadvokaten der anfører, at "det i praksis er problematisk, at der ikke kan foretages hemmelig ransagning [ved efterforskning af grove sager om underslæb, bedrageri, databedrageri, mandatsvig og skyldnersvig]".[15]

På baggrund af denne problematik vil formålet med indførelsen rpl. § 799 blive behandlet, og i den forbindelse vil det blive undersøgt, om strfl. §§ 301, stk. 2, jf. stk. 1 og § 286, stk. 2, jf. 279 a opfylder dette formål.

Ud over at undersøge formålet med rpl. § 799 vil samspillet mellem ransagning, indgreb i meddelelseshemmeligheden, jf. rpl. § 780 og dataaflæsning, jf. rpl. § 791 b, blive behandlet. Almindelig ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning kan foretages ved databedrageri, hvilket ikke er tilfældet ved hemmelig ransagning, hvorfor samspillet mellem indgrebene er relevant at undersøge.

[13] Herefter primært nævnt som skimming

[14] Anker og Jensen, Moderne berigelseskriminalitet - En dybdegående analyse af straffelovens § 279 a, Speciale Københavns Universitet, 2018: http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Prisopgaver/bedste_opg_2018.pdf, (tilgået d. 16/5-19)

[15] Lovudkast L105, 14. oktober 2016, alm. bem., pkt. 2.7.2

"Den teknologiske udvikling og den øgede brug af internettet giver, som det ses, nogle udfordringer, når et straffeprocessuelt tvangsindgreb som hemmelig ransagning skal overføres til en ny digital virkelighed."[16] Ovenstående redegørelse og analyse vil derfor blive foretaget med henblik på at fastlægge, hvorvidt bestemmelsen om hemmelig ransagning er hensigtsmæssig i forbindelse med efterforskning af databedrageri.

Ved IT-kriminalitet kan det være relevant at diskutere det grænseoverskridende element, som ofte indgår i denne type kriminalitet. Imidlertid vil spørgsmålet om jurisdiktion ikke blive behandlet, da dette vil medføre, at de øvrige problemformuleringer kun kunne blive behandlet overfladisk grundet kravene til specialets anslag.

Derudover vil vi ikke behandle strafsanktioner eller andre materielle el. processuelle forhold, end de ovenfor nævnte.

1.3 Metode

Retsdogmatisk metode[17] vil blive anvendt med henblik på at fastlægge dansk retstilstand ud fra emnet retlige udfordringer ved efterforskning og tiltalerejsning i forhold til databedrageri, med det formål at beskrive, analysere og systematisere gældende ret.

For at fastlægge gældende ret vil dette speciale fokusere på dansk straffelov. I den forbindelse vil relevante forarbejderne til bestemmelserne blive behandlet og i den forbindelse inddraget som fortolkningsbidrag.

Inden for det emne som specialet behandler er der et forholdsvis begrænset antal domme. Vi har udvalgt de mest relevante domme, og behandlet disse mere dybdegående i specialet.

For at opnå en dybere baggrundsviden om bestemmelserne har det været nødvendigt at inddrage juridisk litteratur som sekundært fortolkningsbidrag. Den juridisk litteratur er blevet sammenholdt med de øvrige retskilder, for at fastslå at der er overensstemmelse mellem teori og praksis.

[16] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 11
[17] Munk-Hansen, Retsvidenskabsteori, 2014, s. 190

Kapitel 2 - Hvad er internetkriminalitet?

2.1 Begrebet internettet

For at opnå en forståelse af, hvad der karakteriserer internetkriminalitet, er det vigtigt at kunne definere den teknologi der ligger bag og er speciel for denne kriminalitetstype. På denne baggrund vil vi i det følgende afsnit kort definere, hvad der ligger i begreberne internettet og internetkriminalitet ud fra en juridisk synsvinkel.

Der er ikke en definitiv juridisk definition af begrebet internettet. Begrebet kan dog generelt beskrives som: "et verdensomspændende computernetværk af indbyrdes forbundne computernetværk. [Internettet] er summen af det kommunikationsudstyr, der binder millioner af lokalt placerede computere sammen i et netværk."[18]

2.1.1 Internetkriminalitet

Internetkriminalitet er en samlebetegnelse for en lang række forskellige forbrydelser der har det til fælles, at det ved udførelsen af forbrydelsen primært er internettet, og den computerteknologi der knytter sig hertil, som anvendes[19]. Straffelovrådet tog allerede i betænkning nr. 1032/1985 stilling til, hvordan datakriminalitet skulle defineres. De anførte i den forbindelse, at "(...) datakriminalitet er de strafbare handlinger, der rummer en anvendelse af den for databehandling særegne teknik med hensyn til registrering, opbevaring, bearbejdelse og brug af oplysninger. Hertil hører ikke blot uberettiget tilføjelse, ændring eller slettelse af oplysninger, indgreb i dataanlæggets programmering etc., men også det forhold, at en person uden at ændre noget skaffer sig kendskab til oplysninger eller programmer ved uberettiget brug af dataanlægget."[20]

Internetkriminalitet kan generelt inddeles i tre kategorier; computer-integritetsforbrydelser, computer-assisterede forbrydelser og computer-indholdsforbrydelser[21]. Afgørende for opdelingen er måden, hvorpå computeren anvendes til forbrydelsen.

[18] Heine m.fl., Internetjura, 2002, s. 28
[19] Det Kriminalpræventive Råd, Når forbrydelser bliver digitale, marts 2016, s. 10
[20] Betænkning nr. 1032/1985, alm. bem., pkt. 1.2.
[21] Det Kriminalpræventive Råd, Når forbrydelser bliver digitale, marts 2016, s. 10

Computer-integritetsforbrydelser omfatter tilfælde, hvor der sker angreb på andre systemer f.eks. en computer. Eksempler på sådanne angreb kan være hacking[22], computervirus[23], trojanske heste[24]osv. Angrebene kan rette sig mod virksomheder, det offentlige el. private.

Ved computer-assisterede forbrydelser anvendes computerens teknologi som et redskab til at realisere en forbrydelse. Der vil primært være tale om forbrydelser der retter sig mod personer. Eksempler på computer-assisterede forbrydelser er, databedrageri i forbindelse med internethandel, phishing[25] og identitetstyveri[26].

Computer-indholdsforbrydelser omhandler distribuering af ulovligt materiale via internettet. Der kan f.eks. være tale om distribuering af børneporno og voldeligt el. andet racistisk materiale, hvilket er blevet gjort en hel del lettere at udbrede grundet den teknologiske udvikling[27].

[22] Hacking vil sige at en person "uberettiget [skaffer sig] adgang til et informationssystem", jf. Det Kriminalpræventive råd, Når forbrydelser bliver digitale, marts 2016, s. 36

[23] "Computervirus er et program, som kan skade andre programmer. Virus-programmer kan for eksempel slette vigtige data eller programfiler på den inficerede computer. En computervirus skal aktiveres manuelt, ved at bru- geren for eksempel åbner en fil, som vedkommende har tillid til", jf., Det Kriminalpræventive Råd, Når forbrydelser bliver digitale, marts 2016, s. 80

[24] "En trojansk hest er et skadeligt computerprogram (malware), der er gemt i et softwareprogram, som virker godartet, så offeret narres til at downloade programmet", jf. Det Kriminalpræventive råd, Når forbrydelser bliver digitale, marts 2016, s. 82

[25] Phishing er tilfælde hvor gerningspersonen sender en mail der opfordrer offeret til at sende personlige oplysninger eller hvor mailen indeholder et link til en falsk hjemmeside der f.eks. ligner sin banks, jf. Det Kriminalpræventive Råd, Når forbrydelser bliver digitale, marts 2016, s. 82

[26] Identitetstyveri omfatter tilfælde, hvor en persons personlige oplysninger bliver udnyttet, til at opnå en økonomisk vinding, jf. Det Kriminalpræventive Råd, Når forbrydelser bliver digitale, marts 2016, s. 81

[27] Det Kriminalpræventive Råd , Når forbrydelser bliver digitale, marts 2016, s. 10

Kapitel 3 - Afgrænsningen mellem straffelovens §§ 279 og 279 a

3.1 Baggrunden for indførelsen af strfl. § 279 a

I 1985 blev bestemmelsen om databedrageri indført i straffelovens § 279 a[28]. Bestemmelsen minder i sin opbygning og formulering om den almindelige bedrageribestemmelse i strfl. § 279. Grundlaget for indførelsen af denne nye bestemmelse var den teknologiske udvikling der medførte, at der nu gennem computerteknologi kunne foretages bedragerilignende tilfælde, der ikke ville være omfattet af strfl. § 279[29]. Indførelsen af bestemmelsen om databedrageri var derved et resultat af behovet for at kriminalisere tilfælde af bedrageri, hvor processen i høj grad er automatiseret. Ved en automatiseret proces vil vildfarelse af en fysisk person ikke finde sted, men der vil i stedet ske "indgreb i grundlaget for den elektroniske databehandling."[30] Tilfælde, hvor processen primært er automatiseret, vil falde uden for anvendelsesområdet af strfl. § 279, da bedrageri kræver vildledelse af en fysisk person, og at vedkommende som følge heraf foretager en disposition.

Strfl. § 279 skal fortolkes meget udvidende, hvis forhold, hvor processen i overvejende grad er automatiseret, skal kunne indfortolkes herunder. Dette vil udgøre et problem i forhold til legalitetsprincippet i strfl. § 1, der medfører, at straf kun kan pålægges for forhold, der er hjemlet ved lov el. fuldstændig kan ligestilles hermed (fuldstændig analogi)[31]. Der er derved et forbud mod analogislutninger[32], hvilke antages at have haft betydning ved vurderingen af behovet for at indføre bestemmelsen om databedrageri[33]. Derudover antages det også, at

[28] Ved Lov nr. 229, 6. juni 1985
[29] Waaben v/ Langsted, Strafferettens specielle del, 2014, s. 161
[30] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a og LFF 1985-04-24 nr. 221, alm. bem., pkt. 2.3
[31] Betænkning nr. 1417/2002, pkt. 2.6
[32] Dette kan også udledes af Den Europæiske Menneskerettighedskonvention, art. 7, stk. 1, 1. pkt., hvorefter "ingen kan kendes skyldig i strafbar lovovertrædelse på grund af en handling eller undladelse, der ikke udgjorde en strafbar overtrædelse af national eller international ret på den tid, da den blev begået."
[33] "(...) en række bedragerilignende forhold vedrørende dataforhold [vil] falde uden for bestemmelsen [i strfl.] § 279, hvis der ikke i forløbet optræder en person, som er blevet vildledt til at gøre eller undlade noget. [I visse tilfælde kan forholdet da henføres under strfl. §§ 278, stk. 1, nr. 3 eller 280].Ingen af disse bestemmelser er udformet med henblik på at ramme datakriminalitet, og der kan derfor tænkes tilfælde, hvor det vil være mindre naturligt at henføre disse nye kriminalitetsformer under bestemmelserne om pengeunderslæb eller mandatsvig", jf. betænkning nr. 1032/1985, alm. bem., pkt. 6.5

forbuddet har haft indflydelse på at strfl. § 279 a blev formuleret forholdsvis bredt, så nye teknologiske forhold kan subsumeres under bestemmelsen[34].

I nedenstående afsnit vil forskellene mellem de strfl. §§ 279 og 279 a blive behandlet mere dybdegående. På denne måde kommer behovet for at indføre § 279 a i straffeloven til at fremstå tydeligere, og bestemmelsens anvendelsesområde bliver klargjort.

3.2 Straffelovens § 279

Straffelovens § 279 om bedrageri lyder: " For bedrageri straffes den, som, for derigennem at skaffe sig eller andre uberettiget vinding ved retsstridigt at fremkalde, bestyrke eller udnytte en vildfarelse bestemmer en anden til en handling eller undladelse, hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab."

3.2.1 Vildfarelse

En fundamental betingelse for anvendelsen af strfl. § 279 er, at der skal foreligge en vildfarelse hos den der bestemmes til en handling eller undladelse. En vildfarelse kan defineres som en fejlopfattelse, misforståelse eller uvidenhed om noget faktisk eller retligt[35]. Bestemmelsen kan anvendes i de tilfælde, hvor vildfarelsen opstår hos en enkelt person eller en flerhed af personer f.eks. hvor gerningspersonen indrykker en annonce i avisen[36]. Strfl. § 279 forudsætter en uoverensstemmelse mellem gerningspersonen og modpartens opfattelse af grundlaget for en handling eller en undladelse, dvs., at der i handlingsforløbet skal indgå en menneskelig forestilling. Vildfarelse kan foreligge, selvom om den disponerende har en vis tvivl omkring gerningspersonens oplysninger, men hvis mistilliden er for stor, kan der ikke foreligge fuldbyrdet bedrageri[37].

[34] Betænkning nr. 1417/2002, pkt. 2.6, og Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed, hvor det anføres, at, "(...) bestemmelsen blev formuleret så tilpas bredt, at den har været egnet til at rumme den digitale revolutionering, som samfundet har undergået de sidste 20-30 år", jf. s. 2 og "med tanke på den nærmest eksplosive digitale udvikling, der har fundet sted siden – ikke mindst med udbredelsen af internettet – synes loven at være udtryk for en sjælden set rettidig omhu fra lovgivers side", jf. s. 1.
[35] Kommenteret straffelov, Speciel del, 2017, s. 611
[36] Ibid. s. 611
[37] Ibid. s. 611

Efter strfl. § 279 skal vildfarelsen være fremkaldt, bestyrket eller udnyttet af gerningspersonen. Dette kan ske ved, at vedkommende fremsætter positivt urigtige oplysninger eller ved sin aktive adfærd i form af fortielse[38]. Omfattet er også de situationer, hvor gerningspersonen ved sin passivitet retsstridigt udnytter en bestående vildfarelse, der er uafhængig af hans adfærd. Dette viser, at bedrageri også omfatter de tilfælde, hvor gerningspersonen undlader at bringe modparten ud af en vildfarelse[39].

Gerningspersonen skal ved sin handling have bestemt offeret til en tabsvoldende disposition ved fremkaldelse, bestyrkelse eller udnyttelse af offerets vildfarelse. Heri ligger et krav om årsagssammenhæng mellem vildfarelsen og dispositionen. Derudover kræves også årsagssammenhæng mellem gerningspersonens adfærd og dispositionen. Dette vil typisk forekomme i det situationer, hvor udnyttelse foreligger f.eks. hvor gerningspersonen har haft mulighed for at berigtige en vildfarelse, men undlader dette[40]. Kravet om årsagssammenhæng medfører også, at gerningspersonens adfærd skal foreligge inden eller senest samtidig med den disponerendes disposition[41].

3.2.2 Retsstridig

Efter ordlyden af strfl. § 279, er det en forudsætning at fremkaldelse, bestyrkelse eller udnyttelse af en vildfarelse kan karakteriseres som retsstridig. Det kan heraf udledes, at nogle retsforhold vil være straffrie efter bestemmelsen, selvom forholdet lægger sig tæt op af ordlyden i strfl. § 279. Et eksempel på et forhold der ikke er omfattet af strfl. § 279 er, hvor en sælger overdrevet anpriser en vare f.eks. siger, at skoen er uopslidelig[42].

3.2.3 Uberettiget formueforskydelse

Det fremgår af strfl. § 279, at gerningspersonen skal have handlet for at skaffet sig eller andre uberettiget vinding. Denne vinding skal enten resultere i et formuetab eller væsentlig risiko herfor, for den disponerende eller nogen, for hvem handlingen eller undladelsen er afgørende. Begrebet formuetab fortolkes udvidende, hvorfor det også omfatter tilfælde, hvor der foreligger

[38] F.eks. fortielse om insolvens ved oprettelse af lån, jf. Kommenteret straffelov, Speciel del, 2017, s. 611
[39] Kommenteret straffelov, Speciel del, 2017, s. 611
[40] Ibid. s. 612
[41] Ibid. s. 612
[42] Ibid. s. 616

en væsentlig risiko for et ikke-hypotetisk tab[43]. Grænsen skal formentlig trækkes i det tilfælde, hvor den disponerende mister en faktisk udsigt til opnåelse af et formuegode, f.eks. hvis denne ved svig bestemmes til at undlade at foretage en disposition, der kunne have medført en fortjeneste[44].

Det formuetab som indtræder kan enten bestå i en formindskelse af aktiver eller forøgelse af passiver, f.eks. ved optagelse af gæld. Bestemmelsen kræver ikke, at formuetabet eller den væsentlige risiko herfor, indtræder i forbindelse med gerningspersonens disposition. Således vil tilfælde, hvor der ved svig opnås en fuldmagt for at skaffe sig uberettiget vinding på fuldmagtsgiverens bekostning være omfattet, selvom fuldmagtsgiver skal foretage sig yderligere dispositioner for, at et formuetab kan indtræde[45].

Omfattet af begrebet formuetab er også faste ejendomme eller arbejdsydelser, og tabet behøver derfor ikke at være knyttet til en rørlig ting[46].

Formuetabet vurderes på kontraheringstidspunket, hvorfor den disponerende som udgangspunkt kun kan miste formuegoder vedkommende ejer eller har krav på. Tabet vurderes efter dansk ret som udgangspunkt efter et objektivt kriterium dvs. om der rent faktisk foreligger et tab eller risiko for tab. På baggrund af dette foreligger formuetab som udgangspunkt ikke, hvis den disponerende opnår en ydelse, der i værdi svarer til modydelsen[47].

Efter bestemmelsen skal formuetabet være påført den disponerende eller nogen, for hvem handlingen eller undladelsen bliver afgørende. Begrebet nogen omfatter de tilfælde hvor den disponerendes dispositioner rammer andre f.eks. i fuldmagtsforhold[48].

Den tabvoldende disposition kan bestå i en handling eller en undladelse, jf. ordlyden af strfl. § 279. Undladelsen skal være en disposition fra den disponerendes side dvs. et valg om at undlade at handle på en bestemt måde. Tilfælde, hvor en person ikke har kendskab til sit krav og derfor ikke gør det gældende, vil derfor falde uden for bestemmelsens anvendelsesområde[49].

[43] Kommenteret straffelov, Speciel del, 2017, s. 613
[44] Ibid. s. 613
[45] Ibid. s. 613
[46] Ibid. s. 613
[47] Ibid. s. 614
[48] Ibid. s. 615
[49] Ibid. s. 613

3.2.4 Tilregnelse

For at der kan straffes for bedrageri kræves der den fornødne tilregnelse. Subjektivt kræves det, at der er handlet med forsæt til alle elementer i gerningsindholdet. På tidspunktet for vildfarelsens fremkaldelse skal forsættet muligvis allerede være til stede[50].

Ansvar kan derfor være udelukket, hvis personen ikke har været klar over, at den disponerende har befundet sig i en vildfarelse. Dette gælder uanset om personen "selv har svævet i samme vildfarelse (...), eller at vedkommende har troet at modparten handlede med kendskab til samtlige relevante omstændigheder"[51]. Derudover kan ansvar også udelukkes, hvis personen har været klar over, at den disponerende har befundet sig i en vildfarelse, men ikke har indset, at vildfarelsen har været bestemmende for den disponerendes disposition[52].

3.2.5 Fuldbyrdelse

Bedrageri efter strfl. § 279, fuldbyrdes enten når formuetab eller væsentlig risiko herfor, er indtrådt.

3.3 Straffelovens § 279 a

Straffelovens § 279 a, om databedrageri, lyder: "For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling."

3.3.1 Elektronisk databehandling

Begrebet elektronisk databehandling indgår både i 1. og 2. led af strfl. § 279 a om databedrageri og er derved et centralt begreb i bestemmelsen. For at elektronisk databehandling kan finde sted, er det en forudsætning, at der sker anvendelse af et anlæg[53]. Begrebet er ikke defineret nærmere i strfl. § 279 a og er ikke uddybet i forarbejderne til bestemmelsen. I Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet kan der imidlertid hentes inspiration. Det anføres i betænkningen, at elektronisk databehandling sprogligt omfatter "alle oplysninger og enhver form for behandling (...) af oplysninger", som foregår elektronisk[54].

[50] Kommenteret straffelov, Speciel del, 2017, s. 617
[51] Ibid. s. 617
[52] Ibid. s. 617
[53] Ibid. s. 620
[54] Betænkning nr. 1032/1985, alm. bem., pkt. 1.2

Der må udvises tilbageholdenhed med at definere elektronisk databehandling for fast, idet Straffelovrådet i betænkningen[55] har fastlagt en meget bred definition. Dette må antages at være en følge af den teknologiske udvikling, som har medført et behov for en bred formulering så fremtidige forhold er omfattet. Dette er overensstemmelse med Lasse Lund Madsens synspunkt, nemlig, at fordelen ved strfl. § 279 a, 2. led er, at den er "formuleret så tilpas bredt, at den har været egnet til at rumme den digitale revolutionering, som samfundet har undergået de sidste 20-30 år."[56] På grund af denne brede formulering må det være pålagt domstolene at skulle indfortolke, hvad der skal være omfattet af begrebet elektronisk databehandling. Det antages i denne forbindelse, at domstolene vil være tilbøjelige til at følge det almene samfunds forståelse af begrebet[57].

Det fremgår af ovenstående, at elektronisk databehandling er et afgørende element for anvendelsen af strfl. § 279 a. Dette kan give den antagelse, at strfl. § 279 a er uanvendelig så snart der optræder en fysisk person under processen. Sådan forholder det sig imidlertid ikke. Hvis der f.eks. er tale om køb på nettet, hvor en gerningsperson ved uberettiget brug af andres betalingskortoplysninger foretager bestillinger af varer, vil der typisk i slutningen af processen, indgå en lagermedarbejder der pakker og sender varerne. Lagermedarbejderen vil imidlertid pga. sin underordnede stilling ikke foretage en nærmere kontrol af rigtigheden af de i dataanlægget indtastede oplysninger. Derfor må processen på trods af den menneskelige involvering, stadig anses for primært at være automatiseret, hvorfor strfl. § 279 a finder anvendelse[58]. Hvis den menneskelige involvering under processen derved er minimal, pga. personens underordnede stilling, vil strfl. § 279 a finde anvendelse. Dette skyldes, at vedkommende ikke foretager en "reel prøvelse af oplysningernes rigtighed og derfor ikke bliver bragt i bestemmende vildfarelse"[59], hvorfor dette forhold falder uden for anvendelsesområdet af strfl. § 279.

[55] Betænkning nr. 1032/1985
[56] U.2016B.343, s. 2
[57] Greve, EDB-strafferet,1986, s. 16
[58] Betænkning nr. 1032/1985, alm. bem., pkt. 6.3
[59] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a

3.3.2 Fuldbyrdelse

Fuldbyrdelsestidspunktet i strfl. § 279 a, er fremrykket i forhold til almindelig bedrageri efter strfl. § 279. Det fremrykkede fuldbyrdelsesmoment ved strfl. § 279 a, blev anset for nødvendig pga. efterforskningsmæssige hensyn. Straffelovrådet antog, at det ville være "vanskeligt og i nogle tilfælde ligefrem umuligt at fremskaffe nærmere oplysninger om, hvorvidt og i givet fald hvornår den databehandling har fundet sted, i hvilken den ændrede oplysning m.v. er blevet anvendt."[60] I dag synes dette ræsonnement dog forældet. Det vil oftest være muligt med forholdsvis stor tidsmæssig præcision at fastsætte, hvornår den uretmæssige disposition og deraf følgende formuetab har været foretaget, ud fra de elektroniske spor, som gerningspersonen vil efterlade[61].

Fælles for 1. og 2. led i strfl. § 279 a er, at selvom fuldbyrdelsesmomentet fremrykkes kræves det, at økonomisk vinding skal indtræde som umiddelbar følge af de retsstridige handlinger beskrevet i bestemmelsen. Dette betyder, at den økonomiske vinding skal indtræde, uden at gerningspersonen foretager sig yderligere, jf. udtykket "derigennem". Hvis yderligere dispositioner er nødvendige for at vindingen indtræder, kan strfl. § 279 a ikke anvendes, men strfl. § 279 kan muligvis være relevant at inddrage[62]. Dette betyder, at hvis en person f.eks. ikke opnår vinding ved at slette oplysninger til brug for elektronisk databehandling, men efterfølgende modtager et honorar for dette job, vil forholdet ikke være omfattet af strfl. § 279 a[63].

Strfl. § 279 a, 1. led - "ændrer, tilføjer eller sletter oplysninger eller programmer"

Strfl. § 279 a, 1. led, fuldbyrdes allerede når en person med forsæt "ændrer, tilføjer eller sletter oplysninger eller programmer". Det er underordnet, hvorvidt de oplysninger el. programmer som angrebet retter sig mod er lagret eller er ved at blive transmitteret.[64]

Ifølge bestemmelsens 1. led består gerningsindholdet i at "ændre, tilføje eller slette oplysninger eller programmer". Det antages, at formuleringen "ændrer" vil omfatte de fleste forhold, men lovgiver har valgt at supplere med "tilføje eller slette" så bestemmelsens anvendelsesområde

[60] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a
[61] Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed, s. 2-3
[62] Kommenteret straffelov, Speciel del, 2017, s. 620
[63] Greve, EDB-strafferet, 1986 s. 65
[64] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a

fremhæves[65]. Både total og partiel sletning vil herefter være omfattet. Bestemmelsen finder endvidere anvendelse i tilfælde, hvor der indlægges "et nyt supplerende program i dataanlægget"[66], og ved mange andre forhold.

Ved ændring, tilføjelse el. sletning af oplysninger og programmer kræves det ikke, at der er anvendt specifikke metoder. Det er imidlertid et krav, at de oplysninger der skal bruges i den elektroniske databehandling har "nær tidsmæssig (...) nærhed til databehandlingen."[67]

Ændring, tilføjelse eller sletning skal være rettet mod "oplysninger eller programmer til elektronisk databehandling". Der er ikke nogen fastlagt definition af, hvad oplysninger eller programmer er, men grundlæggende må begreberne følge dagligsproget[68].

Knud Waaben anfører, at der er "to grundelementer i en computerbehandling: dens materiale af informationer (oplysninger) og det indlagte programmel, der håndterer behandlingen af disse oplysninger (programmer)"[69] - denne korte definition kan anvendes til at opnå en forståelse af begreberne.

Begrebet programmer er yderligere uddybet i betænkning nr. 1032/1985, hvori det anføres, at "alle operationer bestemmes af programmer, dvs. forud fastlagte instruktioner for ordning, udvælgelse og anden bearbejdelse af data fra computerens lager."[70] Det vil sige, at programmer anses for "selvstændige redskaber til strukturering af datamassen."[71]

Lovgiver har i bestemmelsen valgt at anvende formuleringen oplysninger frem for data, men de to begreber dækker over samme teknologiske fænomen[72]. Vagn Greve fremkommer med en mere uddybende forståelse af data dvs. oplysninger. Han anfører, at data skal forstås som: "enhver form for repræsentation af kendsgerninger eller ideer, der kan kommunikeres eller behandles gennem en eller anden proces."[73]

---

[65] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a
[66] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a
[67] Kommenteret straffelov, Speciel del, 2017, s. 620. Vagn Greve anfører i denne forbindelse, at bestemmelsen ikke finder anvendelse "på enhver oplysning, som på et eller andet tidspunkt i sin senere eksistens vil få karakter af inddata", jf. Greve, EDB-strafferet, 1986, s. 67
[68] Kommenteret straffelov, Speciel del, 2017, s. 620
[69] Waaben v/ Langsted, Strafferettens specielle del, 2014, s. 161.
[70] Jf., alm. bem., pkt. 1.1., denne definition er i tråd med Vagn Greves forståelse af begrebet i EDB-strafferet, 1986, s. 33, hvorefter programmer defineres som: "det sæt af specificerede kommandoer, der direkte eller indirekte styrer og sikrer gennemførelsen af den elektroniske databehandling."
[71] Betænkning nr. 1032/1985, alm. bem., pkt. 1.1.
[72] Carlsen og Elmer, Juristen 1986, Datakriminalitet, s. 295
[73] Greve, EDB-strafferet, 1986, s. 44

Strfl. § 279 a, 2. led - "i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling"
Strfl. § 279 a, 2. led, udvider anvendelsesområdet for bestemmelsen på en forholdsvis bred og ubestemt måde. Der stilles ikke krav mht. måden, hvorpå databehandling påvirkes el. hvilken metode der anvendes til påvirkning. Bestemmelsens 2. led fuldbyrdes således når gerningspersonen "i øvrigt søger at påvirke (...) sådan databehandling", hvilket forudsætter, at dispositionen foretages med berigelsesforsæt og forsæt til at påvirke databehandlingen. Omfattet af 2. led kan f.eks. være tilfælde, hvor der ikke direkte gribes ind i den elektroniske databehandling, men hvor gerningspersonen ændrer oplysninger, som senere skal indtastes af en anden person til den elektroniske databehandling[74].

Passivitet vil kunne være omfattet af bestemmelsens 2. led, men kun, hvis denne passivitet kan sidestilles med en aktiv disposition f.eks. hvor en person undlader at foretage sig noget på trods af, at der er handlepligt[75].

Tilfælde, hvor sletning el. hindring af databehandling er fuldstændig, vil ikke være omfattet af bestemmelsens 2. led[76], da dette ikke ville være i overensstemmelse med ordlyden, hvor der blot skal ske påvirkning af resultatet. Det ville ligeledes være svært at fastslå et forsæt til berigelse i dette tilfælde[77].

3.3.3 Tilregnelse

Fuldbyrdelse af databedrageri kræver subjektivt berigelsesforsæt, jf. formuleringen "for derigennem at skaffe sig eller andre uberettiget vinding". Heri ligger et krav om forsæt til materiel formueforskydning, så der opnås vinding hos gerningspersonen el. tredjemand og deraf følgende adækvat tab hos offeret. Det er imidlertid ikke et krav, at der kan føres bevis for formuetab ved databedrageri[78]. Derudover fremgår det ikke direkte af bestemmelsen, at der skal være forsæt til tabsforvoldelse. Dog antages dette at være tilfældet, da § 279 a er placeret i straffelovens kapitel om formueforbrydelser, og er nævnt som en berigelsesforbrydelse i forarbejderne til bestemmelsen[79]. Vagn Greve anfører, at baggrunden for ikke at have tilføjet

[74] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a
[75] Greve, EDB-strafferet, 1986, s. 67 og betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a
[76] Kommenteret straffelov, Speciel del, 2017, s. 620
[77] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a
[78] LFF 1985-04-24 nr. 221, alm. bem., pkt. 2.4.
[79] Betænkning nr. 1032/1985, de specielle bemærkninger til strfl. § 279 a

kravet om tab i bestemmelsen er, at fuldbyrdelsestidspunktet er fremrykket, og tabsbedømmelsen har således kun betydning i henhold til, om der har forelagt forsæt[80].

Det er uden betydning, hvem der opnår vinding. Der behøver derved ikke at være en forbindelse mellem vedkommende, som udfører den retsstridige disposition og personen, som opnår den deraf følgende vinding. Vindingen kan enten bestå af penge eller goder, der har en økonomisk værdi og behøver ikke at være fysiske ting[81].

Bestemmelsen kræver, at handlingen der foretages er retsstridig. Dette betyder, at forsæt vil være udelukket, hvor sletning af data er lovligt el. hvor en person har anset sig for berettiget til at slette data[82].

3.4 Betydningen af afgrænsningen

Strfl. § 279 a har sit udgangspunkt i strfl. § 279, hvilket har medført, at bestemmelserne har en del lighedstræk. Ifølge Lasse Lund Madsen vil " grænserne [mellem strfl. § 279 og strfl. § 279 a] undertiden være flydende, og det vil i visse situationer nærme sig en slags hjemmelsmæssig smagssag, om man foretrækker den ene bestemmelse frem for den anden. Det vil heller ikke have nogen retlig betydning (...)."[83]

Modsætningsvis kan der argumenteres for, at "en række bedragerilignende forhold vedrørende dataforhold [vil] falde uden for bestemmelsen i § 279, hvis der ikke i forløbet optræder en person, som er blevet vildledt til at gøre eller undlade noget."[84] Sammenholdes dette med legalitetsprincippet, må indførelsen af strfl. § 279 a anses for, at have været vigtig da den medførte, at der var strafhjemmel i tilfælde af bedrageri, hvor der ikke indgår en menneskelig vildfarelse. I den forbindelse er afgrænsningen mellem bestemmelserne meget vigtig, da henførelsen af IT-relaterede bedrageriforhold under strfl. § 279 vil resultere i, at bestemmelsen får et meget bredt anvendelsesområde, som ikke har været tilsigtet.

Lasse Lund Madsen har dog en pointe i, at grænsen ikke er helt fast, idet afgrænsningen afgøres ud fra graden af menneskelig involvering i hændelsesforløbet. Det må derfor i hver sag vurderes, om den menneskelige involvering er dominerende el. processen primært er

[80] Greve, EDB-strafferet, 1986, s. 66
[81] Ibid. s. 65
[82] Ibid. s. 66
[83] U.2016B.343, s. 2
[84] Betænkning nr. 1032/1985, alm. bem., pkt. 6.5

automatiseret. Dette ændrer imidlertid ikke på, at forholdet skal kunne henføres under den rette bestemmelse så der er klar strafhjemmel.

Derudover er det også vigtigt at afgrænse bestemmelserne fra hinanden, idet strfl. § 279 a har et fremrykket fuldbyrdelsesmoment. Databedrageri vil således kunne straffes på et tidligere tidspunkt som en fuldbyrdet forbrydelse, end det er tilfældet ved almindelige bedrageri.

I forbindelse med bevisførelse kan afgrænsningen have betydning, da det ved strfl. § 279 a ikke er påkrævet, at der kan føres bevis for, at offeret har lidt et tab eller væsentlig risiko herfor, modsat strfl. § 279[85].

Selv om bestemmelserne derved har mange fælles kendetegn, har de også nogle unikke kendetegn der er afgørende for, hvordan de afgrænses over for hinanden.

Kapitel 4 - Afgrænsningen mellem straffelovens §§ 276 og 279 a

4.1 Kendetegn ved strfl. § 276

I den juridiske litteratur er afgrænsningen mellem strfl. §§ 276 og 279 a blevet diskuteret[86]. Diskussionen har omhandlet, hvorvidt strfl. § 279 a har været fortolket for indskrænkende i forhold til sit anvendelsesområde. Som følge heraf, er strfl. § 276 formodentlig blevet anvendt i en videre udstrækning end tilsigtet, da forhold som kunne være henført under strfl. § 279 a, muligvis er blevet henført under strfl. § 276.

I ovenstående afsnit er de specielle kendetegn, der karakteriserer strfl. §§ 279 og 279 a blevet gennemgået. I dette afsnit vil de kendetegn der gælder for strfl. § 276 blive behandlet. Dernæst vil der blive foretaget en undersøgelse af, hvorvidt afgrænsningen mellem strfl. §§ 276 og 279 a overhovedet medfører eller har medført problemer, og i så fald, hvilken betydning dette har.

Strfl. § 276 lyder: "For tyveri straffes den, som uden besidderens samtykke borttager en fremmed rørlig ting for at skaffe sig eller andre uberettiget vinding ved dens tilegnelse. Med

[85] LFF 1985-04-24 nr. 221, alm. bem., pkt. 2.3 og Carlsen og Elmer, Juristen 1986, Datakriminalitet, s. 298
[86] Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed

rørlig ting sidestilles her og i det følgende en energimængder, der er fremstillet, opbevaret eller taget i brug til frembringelse af lys, varme, kraft eller bevægelse eller i andet økonomisk øjemed."

4.1.1 Fremmed rørlig ting

Det fremgår af strfl. § 276, at forbrydelsens genstand er en fremmed rørlig ting. Begrebet må forstås som en fysisk genstand der kan flyttes, hvilket betyder, at uberettiget brug af opfindelse, navn mv., ikke skal anses for at være tyveri[87].

Det er en betingelse, at genstanden er i en anden persons varetægt dvs. tilhører en anden end gerningspersonen[88], jf. "fremmed". Der stilles krav om, at tingen borttages uden besidderens samtykke, da borttagelse med samtykke ikke vil være uberettiget, og det derfor ikke vil give mening at statuere tyveri[89]. Besidderen skal være i stand til at overskue konsekvenserne af et samtykke[90]. Hvis samtykke f.eks. er opnået gennem svig eller udnyttelse vil strfl. § 276 ikke finde anvendelse, men strfl. § 279 kan eventuelt være relevant. Afgørende for at ifalde ansvar er, hvad personen der borttager genstanden har haft forsæt til - hvis vedkommende troede at der var gyldig tilladelse til at borttage tingen, vil tyveri være udelukket[91].

4.1.2 Fuldbyrdelse

Tyveri efter strfl.§ 276 fuldbyrdes ved borttagelse af den fremmede rørlige ting, dvs. når tingen "egenmægtigt fjernes fra det sted, hvor den befinder sig."[92] Dette kræver normalt, at der er fysisk kontakt mellem genstanden og gerningspersonen, men uansvarligt mellemled kan eventuelt anvendes til borttagelsen[93]. Der skal meget lidt til, før der statueres borttagelse. Således vil det forhold, hvor gerningspersonen tager penge fra en disk i en butik, lægger dem i sin lomme og sammenblander dem med egne midler, kunne blive betragtet som borttagelse -

[87] Kommenteret straffelov, Speciel del, 2017, s. 587
[88] Ibid. s. 587
[89] Det kan dog være relevant at statuere anden forbrydelse, da f.eks. samtykke fra besidder der ikke ejer ting kan udgøre et forhold af medvirken til underslæb eller hæleri, jf. Kommenteret straffelov, Speciel del, 2017, s. 595
[90] Kommenteret straffelov, Speciel del, 2017, s. 595
[91] Ibid. s. 595
[92] Ibid. s. 594
[93] Ibid. s. 594

borttagelsen består derved i den blotte håndbevægelse[94]. Fuldbyrdelse sker således på et tidligt tidspunkt.

4.1.3 Tilregnelse

Borttagelse skal ske med henblik på tilegnelse, dvs. gerningsperson skal have forsæt til at betragte og råde over tingen som var det vedkommendes egen. "Tilegnelse består [således] i at udøve en ejers beføjelser og bringe den retmæssige ejers råden til ophør"[95], gennem faktisk og retlig råden. Derfor vil borttagelse med midlertidigt brug for øje, el. med det formål at ødelægge tingen, ikke være tyveri[96].

Tilegnelse skal ske med det formål at "skaffe sig eller andre uberettiget vinding". Dette udledes af, at strfl. § 276 er en berigelsesforbrydelse, hvorefter der kræves berigelsesforsæt fra gerningspersonens side dvs. forsæt til vinding for gerningspersonen selv eller andre, og et deraf følgende tab for offeret. Subjektivt kræves at gerningspersonen har haft forsæt til alle led i forbrydelsens gerningsindhold på tidspunktet for borttagelsen[97].

Da tyveri derved kræver berigelsesforsæt, må den genstand der borttages nødvendigvis også skulle have en økonomisk værdi. Traditionelt tillagde man begrebet økonomisk værdi den betydning, at tingen skulle have en "almindelig byttеværdi"[98] efter en standard vurdering[99]. I retspraksis statueres der dog også tyveri, hvor genstanden har en "klar omsætningsværdi på det »åbne« illegale marked"[100] (f.eks. ved kreditkort, narko osv.), jf. f.eks. TfK 2009.48 Ø[101].

4.2 Indskrænkende fortolkning af strfl. § 279 a

I dette afsnit vil det blive undersøgt om anklagemyndighedens tiltalerejsning ved tyveri og misbrug af betalingskort har medført, at strfl. § 279 a om databedrageri, har fået et for snævert anvendelsesområde pga. tvivl om bestemmelsens udstrækning.

---

[94] Waaben v/ Langsted, Strafferettens specielle del, 2014, s. 118
[95] Ibid. s. 127
[96] Det vil derimod kunne henføres under strfl. §§ 293 eller 291, om henholdsvis brugstyveri og hærværk, jf. Kommenteret straffelov, Speciel del, 2017, s. 595-596
[97] Kommenteret straffelov, Speciel del, 2017, s. 597
[98] Ibid. s. 590
[99] Ibid. s. 590
[100] Ibid. s. 590
[101] Dommen omhandlede tyveri af dankort

Ifølge Lasse Lund Madsen har bestemmelsen om databedrageri ikke altid har været anvendt i sin fulde udstrækning. Han anfører, at "anklagemyndigheden, navnlig frem til dommen U 2014.1688 V, anlagde en indskrænkende fortolkning af bestemmelsen, der i en årrække gjorde, at § 279 a ikke blev benyttet i det omfang, kriminalitetsbilledet rent faktisk tilsagde."[102] Denne praksis tilskriver han i høj grad Vagn Greve. Baggrunden for dette er, at Vagn Greve ved udarbejdelsen af den Kommenteret straffelov[103] fremførte sit synspunkt omkring afgrænsningen mellem strfl. §§ 276 og 279 a. Han anførte således i kommentarerne til strfl. § 279 a, at "(...) det stadig [var] det retteste at anvende tyveribestemmelsen på personer, som ved uberettiget brug af andres betalingskort får benzin på en automatisk tank eller penge i en automat"[104]. Denne passus mener Lasse Lund Madsen har haft betydning for anklagemyndighedens tiltalerejsning, da han påpeger, at den Kommenteret straffelov[105] "for de fleste anklagere er det ledende opslagsværk, når det kommer til afklaring af strafferetlige problemstillinger."[106] Sammenholdes dette med, at Vagn Greve som professor i strafferet valgte at anvende ordet "retteste" i den Kommenteret straffelov[107], tilslutter vi os, at dette kan have haft en særlig særlig autoritativ indflydelse på den anklager, der har skulle rejse tiltale.

Vagn Greve understøttede bl.a. sit synspunkt med dommene U 2001.1980/2H og TfK 2009.48 Ø. I U 2001.1980/2H[108] blev subsumptionsspørgsmålet imidlertid slet ikke prøvet, da hovedspørgsmålet i sagen angik strafudmåling ved drab på tidligere samlever. Dommen virker derfor irrelevant, da domstolene ved tiltalerejsningen ikke blev opfordret til at tage stilling til spørgsmålet om subsumption, eftersom der kun var rejst tiltale efter strfl. § 276.

Dommen TfK 2009.48 Ø var et resultat af anklagemyndighedens hidtidige praksis angående tiltalerejsning. Sagen angik afluring og tyveri af dankort der herefter blev anvendt til uretmæssige hævninger, samt forsøg herpå. Hele hændelsesforløbet blev ved tiltalerejsning henført under strfl. § 276, selvom den efterfølgende anvendelse af dankortene i stedet for kunne have været henført under databedrageri efter strfl. § 279 a. Anklagemyndighedens

[102] U.2016B.343, s. 1
[103] Kommenteret straffelov, Speciel del, 2012
[104] Kommenteret straffelov, Speciel del, 2012, s. 545, dette synspunkt blev allerede fremhævet af Vagn Greve i EDB-strafferet, 1986, s. 70
[105] Kommenteret straffelov, Speciel del, 2012
[106] U.2016B.343, s. 3. Dette baserer han på sin praktiske erfaring som tidligere anklager. Fremgangsmåden virker fornuftig, da den Kommenterede straffelov kan udgøre et vigtigt fortolkningsbidrag ved tvivl om juridiske problemstillinger.
[107] Kommenteret straffelov, Speciel del, 2012
[108] Tiltalte blev tiltalt for tyveri, jf. strfl. § 276, for at stjæle samlevers kort og anvende det i dankortautomater

tiltalerejsning fulgte Vagn Greves synspunkt om, at tilfælde hvor "(...) personer, (...) ved uberettiget brug af andres betalingskort får (...) penge i en automat"[109], skal henføres under strfl. § 276 om tyveri.

Straffelovrådet åbnede dog allerede i betænkning nr. 1032/1985 op for, at "der [muligvis kunne] tænkes at blive statueret tyveri i tilfælde, hvor en person opnår udbetaling af penge i en bank med et EDB-styret pengeudbetalingssystem, idet han i maskinen anvender et falsk hævekort. Tilfældet har en vis lighed med det fra den før-elektroniske tid kendte forhold, at en person tilegner sig varer fra en automat ved at indkaste en falsk mønt eller et møntformet metalstykke. Dette anses som tyveri, idet udløsning af automatens mekanik er et middel til at borttage varer."[110]

Det blev fremhævet af Straffelovrådet, at tyveribestemmelsen *muligvis* kunne anvendes ved hævninger med falsk hævekort, og der blev ikke taget stilling til tilfælde, hvor ægte stjålne hævekort anvendes[111]. Denne sondring fremhæves ikke af Vagn Greve, da han primært fokuserede på, om der skete en egenmægtig tilegnelse i handlingsforløbet. Han anførte således, at "det er ligegyldigt for den juridiske bedømmelse, om automaten åbnes ved hjælp af et brækjern eller af en værdiløs metalskive (…) det gør ingen forskel heri, at låsen til pengeskabet er elektronisk."[112] Vagn Greve tillagde derved selve tilegnelsen af pengene større betydning end den forudgående kriminelle metode til at opnå dette mål.

Lasse Lund Madsen tilslutter sig ikke Vagn Greves argumentation, idet han fremhæver at det centrale ved databedrageri er den retsstridige påvirkning af elektronisk databehandling der sker ved hævning i automat[113]. Lasse Lund Madsen mener derved ikke, at det er afgørende for subsumptionen, at der ved hævning sker borttagelse af en fremmed rørlig ting i form af kontanter[114]. Dette anses for at være i overensstemmelse med Straffelovrådets synspunkt, da de heller ikke anser borttagelsen af en fremmed rørlig ting for at være det centrale i databedrageri. De konluderer således at "(...) kravet om borttagelse af en fremmed rørlig ting i § 276 [formentlig] giver tyveribestemmelsen et meget mindre anvendelsesområde i dataforhold end bestemmelserne om brugstyveri, bedrageri og mandatsvig. Der ses ikke at være noget behov for ved lovændring at udvide tyveribestemmelsens område med henblik på

[109] Kommenteret straffelov, Speciel del, 2012, s. 545
[110] Betænkning nr. 1032/1985, alm. bem., pkt. 3.2
[111] Ibid. alm. bem., pkt. 3.2
[112] Greve, EDB-strafferet, 1986, s. 70
[113] U.2016B.343, s. 6
[114] U.2016B.343, s. 6

dataforhold."[115] Ud fra Straffelovrådets konklusion kan der derfor stilles spørgsmålstegn ved, hvorfor Vagn Greve ved sin kommentar udvidede anvendelsesområdet for strfl. § 276, til at omfatte misbrug af betalingskort.

4.2.1 Ændring i tiltalepraksis

Indtil dommen U 2014.1688 V[116] havde anklagemyndigheden rejst tiltale efter strfl. § 276 i tilfælde, hvor hævekort var blevet misbrugt i pengeautomater. Subsumptionsspørgsmålet i henhold til henførelsen af forholdet under strfl. §§ 276 eller 279 a, var ikke før blevet prøvet af domstolene.

I U 2014.1688 V nedlagde anklagemyndigheden i 1. instans påstand om straf efter strfl. § 279 a om databedrageri og opnåede dom herfor. Ved sagens behandling i landsretten ændrede statsadvokaten dog pludselig subsumptionsspørgsmålet, idet han subsidiært nedlagde påstand om straf efter strfl. § 276. En repræsentant fra statsadvokaten tilkendegav i denne forbindelse, "at byretsdommen formentlig var forkert, idet tyveribestemmelsen måtte være rette strafhjemmel."[117] Denne ændring af tiltalen gav anledning til, at landsretten var nødsaget til at behandle subsumptionsspørgsmålet. I den forbindelse anførte landsretten, at "særligt bemærkes det vedrørende spørgsmålet, om forholdet må anses for databedrageri efter straffelovens § 279 a eller tyveri efter straffelovens § 276, at uberettiget brug af et kort og en terminal til hævning som udgangspunkt er omfattet af straffelovens § 279 a (...). Ved en sådan transaktion sker der påvirkning af resultatet af elektronisk databehandling og dermed indgreb i grundlaget herfor. Derimod indebærer denne form for datakriminalitet typisk ikke, som ved tyveri, borttagelse af en fremmed rørlig ting (...)". Landsrettens begrundelse fastslog grænserne mellem strfl. §§ 276 og 279 a. Dommen tydeliggjorde derved, at databedrageri er den rette bestemmelse i forbindelse med misbrug af betalingskort i hæveautomater.

---

[115] Betænkning nr. 1032/1985, alm. bem., pkt. 3.2. Problematikken omkring Vagn Greves og Straffelovrådets synspunkter behandles af Lasse Lund Madsen i U.2016B.343, Bedrageri i den digitale virkelighed, s. 3

[116] Dommen omhandlede 4 personer T1-T4, der blev fundet skyldige i overtrædelse af strfl. § 286, stk. 2, jf. § 279 a, dvs. databedrageri af særlig grov beskaffenhed. En række uidentificerede personer havde oprettede firmaer, og i den forbindelse indgået aftaler med Nets, for at få udleveret dankortterminaler. "Terminalerne blev benyttet til at overføre store pengebeløb ved brug af dankort, der typisk var stjålne eller stillet til rådighed til formålet. Beløbene blev dernæst kort tid efter videreoverført til forskellige konti, hvorfra de blev hævet og i visse tilfælde anvendt til at købe guld."

[117] Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed, s. 5

Nyere tiltalepraksis følger præmisserne i U 2014.1688 V. Således blev der i TfK 2015.443 Ø, rejst tiltale efter strfl. § 290, stk. 1, for at have "modtaget et stjålet Visa/Dankort", og efter strfl. § 276, for at have "misbrugt det til hævninger (...)". Med hensyn til tiltalen efter strfl. § 276 for de uberettigede hævninger, fulgte anklagemyndigheden tiltalepraksis før U 2014.1688 V. Ved hovedforhandlingens begyndelse ønskede anklagemyndigheden imidlertid at henføre forholdet under strfl. § 279 a. Dette nægtede byretten, hvorefter anklageren kærede beslutningen. Anklagemyndigheden anførte i kæreskriftet, "at uberettiget brug af et dankort og en terminal til hævning efter Vestre Landsrets dom [U 2014.1688 V] skal anses som databedrageri efter straffelovens § 279 a (...)". Anklagemyndigheden fulgte derved landsrettens begrundelse og resultat i U 2014.1688 V, og berigtigelsen af tiltalen blev tilladt.

TfK 2015.590 V[118] og TfK 2015.653 V[119] understøtter også, at anklagemyndigheden følger den ændrede tiltalepraksis efter U 2014.1688 V. I disse domme blev der således rejst tiltale efter strfl. § 279 a for anvendelsen af betalingskort til uberettigede hævninger.

Lasse Lund Madsen fremhæver en dom fra retten i Glostrup fra d. 11. marts 2015[120], hvor retten ikke følger tiltalepraksis efter U 2014.1688 V. Sagen omhandlede et tilfælde, hvor flere i forening havde afluret betalingskortkoder, stjålet og efterfølgende brugt de pågældende kort med rette koder til at få udbetalt penge[121]. Anklagemyndigheden rejste tiltalte efter strfl. § 276 for det indledende tyveri af betalingskort, og strfl. § 279 a for den efterfølgende anvendelse. Derved fulgte de tiltalepraksis efter U 2014.1688 V, for så vidt angår henførelsen af uberettiget brug af betalingskort under strfl. § 279 a. Det specielle ved denne dom er imidlertid, at retten af egen drift subsumerede hele hændelsesforløbet under strfl. § 276 med den begrundelse, at "de tiltalte [havde] brugt kortene med rette kode og (...) derved fået udbetalt de omhandlede

[118] T1 og T2 havde "[påmonteret] teknisk udstyr bestående af en falsk front på betalingskortautomat, som kopierede og gemte kortoplysninger og pinkoder på de kunder, der anvendte terminalen", dvs. de havde opsat skimmingudstyr. For dette forhold blev de dømt efter strfl. § 301, stk. 2, jf. stk. 1, nr. 1, da det var foregået over flere omgange, og de havde forsæt til uberettiget at anvende oplysningerne "som identificere et betalingsmiddel, der er tildelt andre". Derudover blev de fundet skyldige i overtrædelse af strfl. § 279 a, jf. § 286, stk. 1, da de kopierede 105 betalingskort, og sendte kortoplysningerne samt pinkoder til medgerningsmænd i USA, der foretog hævninger, hvorved Nets Danmark led et økonomisk tab på 232.578 kr. T1 og T2 blev ligeledes fundet skyldige i forsøg på overtrædelse af § 279 a, jf. § 286, stk. 2, da de havde forsøgt at hæve 289.223 kr. på kortene.
[119] T havde alene og sammen med andre stjålet flere dankort, som blev anvendt til uberettigede hævninger ved brug kortenes pinkoder, som de havde afluret. T blev tiltalt for tyveri, jf. strfl. § 276 for det indledende tyveri af dankortene, mens T for de efterfølgende uberettigede hævninger blev tiltalt for databedrageri efter strfl. § 279 a.
[120] U.2016B.343, s. 6. Se Bilag 3
[121] Bilag 3

pengebeløb. Der er herved i modsætning til de forhold, der var under pådømmelse i U 2014.1688 V, sket borttagelse af en fremmed rørlig ting, hvorfor forholdene findes at skulle henføres under straffelovens § 276."[122]

Lasse Lund Madsen mener, at dette er en fejlslutning af præmisserne i U 2014.1688 V. Præmisserne fastslår netop, at det centrale ved misbrug af betalingskort til hævning i automat er påvirkning af elektronisk databehandling[123]. Ovenstående domme ser ud til at følge tiltalepraksis efter U 2014.1688 V. Den Kommenteret straffelov fra 2017[124] understøtter ligeledes den ændrede tiltalepraksis, da det nu fremgår at "for så vidt angår personer, som ved uberettiget brug af andres betalingskort får (...) penge i en automat, taler U 2014.1688 V for at anvende § 279 a."[125] På baggrund af dette anses Retten i Glostrup for, at have fejlfortolket afgrænsningen mellem strfl. §§ 276 og 279 a.

4.2.2 Straf i sammenstød ved strfl. §§ 276 og 279 a

I ovenstående afsnit er problematikken om subsumption behandlet i henhold til strfl. §§ 276 og 279 a, ved uberettigede hævninger med betalingskort. Spørgsmålet er imidlertid, om der kan straffes i sammenstød ved strfl. §§ 276 og 279 a. Dette spørgsmål er relevant i de situationer, hvor der indledende begås tyveri af betalingskort og efterfølgende sker anvendelse af dette kort til uberettigede hævninger i hæveautomat.

Lars Bo Langsted anfører at "tyveri af et kort (...) som udgangspunkt [vil] kunne straffes som tyveri (§ 276) i sammenstød med §§ 280/279/279 a for den senere anvendelse."[126] Dette har også støtte i retspraksis, jf. bl.a. TfK 2015.653 V og TfK 2015.289 Ø[127] .

Lasse Lund Madsen diskuterer også forholdet omkring straf i sammenstød, hvis både tyveri og databedrageri indgår i hændelsesforløbet[128]. I den forbindelse behandler han spørgsmålet omkring, hvilken bestemmelse forholdet skal subsumeres under, hvis der ikke skal straffes i

[122] Bilag 3
[123] U.2016B.343, s. 6
[124] Kommenteret straffelov, Speciel del, 2017
[125] Kommenteret straffelov, Speciel del, 2017, s. 619-620
[126] U.2019B.48, s. 3
[127] T1 var ansat ved Københavns Postcenter, hvor han stjal tre forsendelser, hvoraf den ene indeholdt et Visa/Dankort - for dette forhold blev T1 fundet skyldig efter § 276. Derudover blev T1 fundet skyldig i overtrædelse af strfl. § 263, stk. 1, nr. 1, "ved at have brudt de forsendelser, hvori kortene lå." T1 anvendte Visa/Dankortet til at bestille en rejse hos Spies A/S, til en værdi af 53.600, hvilket medførte et tab hos Spies A/S. Benyttelsen af kortet udgjorde en overtrædelse af § 279 a.
[128] U.2016B.343

sammenstød. Han anfører, at det ved valget mellem strfl. §§ 276 og 279 a "synes (...) mere oplagt samlet at henføre forholdene under § 279 a, idet det er her tyngden i den kriminelle gerning ligger. For så vidt er det indledende tyveri af hævekortet blot et middel til at opnå selve målet, nemlig den efterfølgende retsstridige hævning af kontanter."[129] Baggrunden for denne betragtning finder han i lex specialis-grundsætningen der "taler (...) for at anvende § 279 a, eftersom bestemmelsen blev indført for at sikre en klar hjemmel ved bedragerier, hvor der ikke umiddelbart fandt en menneskelig vildledning sted."[130] Synspunktet ser ud til at være i overensstemmelse med dommen U 2014.1688 V, hvor hele hændelsesforløbet, herunder det indledende tyveri af hævekort, blev henført under strfl. § 279 a. Som anført følger anklagemyndigheden tiltalepraksis i dommen ved, at uberettiget brug af hævekort i automat nu henføres under strfl. § 279 a. Imidlertid følger anklagemyndigheden ikke tiltalepraksis i dommen med hensyn til at subsumere hele hændelsesforløbet under strfl. § 279 a. Således viser retspraksis[131], at der rejses tiltale både for det indledende tyveri af dankortet og databedrageri for den efterfølgende anvendelse, hvorved der straffes i sammenstød ved strfl. §§ 276 og 279 a. Dette antages at give et overblik over forbrydelsens forløb og derved afgrænse bestemmelsernes anvendelsesområde over for hinanden.

4.3 Betydningen af afgrænsningen

Dommen U 2014.1688 V fastslog, hvordan strfl. §§ 276 og 279 a skulle afgrænses i forhold til hinanden, ved uberettigede hævninger i automat med betalingskort. Som nævnt anvendte anklagemyndigheden forud for dommen tyveribestemmelsen på disse forhold, hvilket gav anledning til en indskrænket anvendelse af strfl. § 279 a. Omvendt resulterede tidligere tiltalepraksis i, at strfl. § 276 fik et bredere anvendelsesområde end tilsigtet. Før U 2014.1688 V, blev tyveribestemmelsen derved anvendt på forhold, hvor strfl. § 279 a kunne havde fundet anvendelse. Grundlaget for denne fejlfortolkning kan muligvis skyldes, at anklagemyndigheden har fulgt Vagn Greves kommentar til strfl. § 279 a i den Kommenteret straffelov[132].

Fejlfortolkningen af strfl. § 279 a har medført, at bestemmelsen ikke har været anvendt i sin fulde udstrækning. Grundet den indskrænkede anvendelse af strfl. § 279 a kan det være

[129] U.2016B.343, s. 4
[130] Ibid. s. 4
[131] Jf. TfK 2015.653 V og TfK 2015.289 Ø
[132] Kommenteret straffelov, Speciel del, 2012

problematisk at fastlægge hvornår databedrageri blev et samfundsmæssigt problem. Dette kan have haft betydning for indsatsen med at forebygge denne type kriminalitet. Da databedrageri foregår på internettet, kan det derfor være nødvendigt med andre efterforskningsskridt end ved traditionel kriminalitet som tyveri[133].

Afgrænsningen har også betydning, ud fra retssikkerhedsmæssige overvejelser. Det er ikke altid oplagt at anvende de traditionelle berigelsesforbrydelser - i det her tilfælde strfl. § 276 - ved IT-kriminalitet. Ved at subsumere det kriminelle forhold under den rette paragraf, får bestemmelserne deres tilsigtede anvendelsesområde. Derudover fremstår strafhjemlen også klarere, end hvis de traditionelle berigelsesforbrydelser skal udvides uforholdsmæssigt til at omfatte IT-kriminalitet.

Endvidere må en ensretning i tiltalepraksis og retspraksis også tilstræbes, for at opnå en entydig og gennemskuelig anvendelse af bestemmelserne. En ensretning i tiltalepraksis og retspraksis vil ligeledes tydeliggøre omfanget af problemet med IT-kriminalitet. Derved vil der også være bedre grobund for ensartet og effektiv forebyggelse af denne type kriminalitet.

4.4 Straffelovens § 301

Forud for databedrageri kan der i stedet for tyveri af et fysisk betalingskort ske anskaffelse mv. af betalingskortoplysninger. Da formålet med overtrædelse af henholdsvis strfl. §§ 276 og 301 i begge tilfælde kan være databedrageri, er det interessant at undersøge om samspillet mellem strfl. §§ 301 og 279 a adskiller sig fra samspillet mellem strfl. §§ 276 og 279 a - dvs. om der straffes i sammenstød i begge tilfælde.

Straffelovens § 301 lyder: " Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der med forsæt til uberettiget anvendelse fremstiller, skaffer sig, besidder eller videregiver

1) oplysninger, som identificerer et betalingsmiddel, der er tildelt andre, eller
2) generede betalingskortnumre

Stk. 2. Sker den i stk. 1 nævnte videregivelse m.v. i en videre kreds eller under særligt skærpende omstændigheder, er straffen fængsel indtil 6 år

Stk. 3. Bestemmelsen i stk. 1 finder ikke anvendelse på ægte betalingskort."

[133] https://politi.dk/rigspolitiet/nyhedsliste/nyt-center-skal-bekaempe-it-relateret-oekonomisk-kriminalitet/2019/01/08, (tilgået d. 16/5-19). I 2019 blev LCIK (Landsdækkende Center mod It-relateret økonomisk Kriminalitet) oprettet. Oprettelsen af dette center viser, at der er et behov for en specialiseret indsats mod IT-kriminalitet.

Strfl. § 301 blev indført i 2004 på baggrund af betænkning nr. 1417/2002 om IT-kriminalitet. I betænkningen blev det vurderet, at "både produktion, forskaffelse, besiddelse med henblik på uberettiget brug og videregivelse af falske betalingskort [burde] kriminaliseres"[134]. Formålet med indførelsen af strfl. § 301 var, at sikre at der er en klar strafhjemmel ved produktion mv. af betalingskortoplysninger - og derved sikre samfundet mod misbrug af betalingskort[135].

4.4.1 Betalingskortoplysninger

Efter bestemmelsens ordlyd omfatter den brug af betalingskortoplysninger f.eks. kortnumre, der gør, at besidderen kan foretage betalinger fra en andens konto[136]. Ægte betalingskort er ikke omfattet af bestemmelsen, jf. strfl. § 301, stk. 3.

Det fremgår af bestemmelsen, at de strafbare handlinger "består i at fremstille, skaffe sig, besidde eller videregive de nævnte oplysninger"[137] som identificerer et betalingsmiddel. Ved fremstilling af oplysninger kan dette ske ved enten forfalskning eller ved genererede betalingskortnumre[138]. Genererede numre defineres som " betalingskortnumre, der skabes via elektronisk behandling på baggrund af matematiske modeller, og som medfører, at betalingskortnummeret fremtræder som gyldigt."[139] Kortnumre der er konstrueret frit er også omfattet af bestemmelsen[140].

Det er uden betydning for bestemmelsens anvendelse, om kortnumrene henviser til et falsk kort, eller om der ikke eksisterer et fysisk kort[141]. Imidlertid vil anvendelsesområdet for strfl. § 301 typisk omfatte "konstruerede eller eftergjorte betalingsmidler, herunder hvide kort[142] med eftergjort magnetstrimmel."[143]

[134] Betænkning nr. 1417/2002, pkt. 8.6.2.
[135] Kommenteret straffelov, Speciel del, 2017, s. 711
[136] Ibid. s. 711
[137] Ibid. s. 711
[138] Ibid. s. 711
[139] LFF 2003-11-05 nr. 55, alm. bem., pkt. 3.2.2
[140] Kommenteret straffelov, Speciel del, 2017, s. 712
[141] Ibid. s. 712
[142] Et hvidt kort karakteriseres som et kort, hvor oplysninger overføres til magnetstriben. jf. betænkning nr. 1417/2002, pkt. 4.3.1
[143] Kommenteret straffelov, Speciel del, 2017, s. 712

Hvor den strafbare handling består i at skaffe sig oplysninger om andres kort angår det typisk ægte kort[144]. Dette bliver ofte betegnet som skimming hvor en eller flere gerningsmænd påmonterer en falsk front og et kamera på en betalingsautomat, som kopierer magnetstriben og pinkode fra kort der bliver anvendt i maskinen[145]. Gerningsmanden kan derved indsamle kortoplysninger og overføre dem til et hvidt kort på størrelse med et almindeligt betalingskort[146].

4.4.2 Fuldbyrdelse

Da strfl. § 301 består af fire forskellige strafbare handlinger medfører dette, at bestemmelsen har fire fuldbyrdelsestidspunkter. Fuldbyrdelse kan derved indtræde på forskellige tidspunkter[147].

Bestemmelsen kriminaliserer også besiddelsen af oplysninger. "Selv om besiddelse typisk [må anses for at] indgå i [hændelsesforløbet ved] produktion, forskaffelse og videregivelse, [er dette dog medtaget for] at undgå fortolkningsproblemer vedrørende besiddelse."[148]

Brugen af betalingskortoplysninger vil kunne karakteriseres som bedrageri, jf. strfl. § 279 eller databedrageri, jf. § 279 a. Anskaffelsen vil i forbindelse hermed udgøre forsøg på strfl. §§ 279 eller 279 a[149]. For at der kan straffes for forsøg efter strfl. §§ 279 eller 279 a kræves der dog, at forsættet er konkretiseret[150], hvilket ikke altid er tilfældet. I tilfælde, hvor forsættet til uberettiget anvendelse ikke er konkretiseret, vil strfl. § 301 således finde anvendelse, da bestemmelsen har et fremrykket fuldbyrdelsesmoment, hvorefter selve anskaffelsen af betalingskortoplysninger er strafbelagt. Dette begrundes med, "at der ikke er nogen rimelig interesse i at kunne skaffe sig eller videregive disse oplysninger ud over i relevante erhvervsmæssige sammenhænge."[151]

[144] Kommenteret straffelov, Speciel del, 2017, s. 712
[145] Langsted, U.2019B.48, Dankortet i strafferetlig belysning, s. 4
[146] Ibid. s. 4
[147] Kommenteret straffelov, Speciel del, 2017, s. 712
[148] LFF 2003-11-03 nr. 55, alm. bem., pkt. 3.3.2
[149] Kommenteret straffelov, Speciel del, 2017, s. 711
[150] Waaben v/ Langsted, Strafferettens almindelige del I, Ansvarslæren, 2011, s. 223-225
[151] Kommenteret straffelov, Speciel del, 2017, s. 711

4.4.3 Tilregnelse

Det er en forudsætning for anvendelse af strfl. § 301 at der subjektivt har været forsæt til uberettiget anvendelse, jf. bestemmelsens ordlyd. Imidlertid skal forsættet til den uberettigede anvendelse ikke være konkretiseret[152].

4.5 Straf i sammenstød ved strfl. §§ 301 og 279 a

Indledende forbrydelse efter strfl. § 301 vil ofte udvikle sig til bedrageri eller databedrageri. Derfor er det vigtigt for afgrænsningen at vurdere om der kan straffes i sammenstød ved strfl. §§ 301 og 279 a. Ifølge juridisk litteratur er der ikke tvivl om, at der kan straffes i sammenstød ved fuldbyrdet overtrædelse af strfl. §§ 301 og 279 a[153]. Spørgsmålet er imidlertid, om der skal straffes for forsøg på databedrageri i sammenstød med fuldbyrdet realisering af strfl. § 301.

Lars Bo Langsted anfører, at der kan straffes i sammenstød med de to bestemmelser. I en sag omhandlende opsætning af skimmingudstyr vil der da kunne straffes for besiddelse af hvide kort efter strfl. § 301, og anvendelsen af kortene vil kunne straffes efter strfl. § 279 a. Ifølge Lars Bo Langsted kan der dømmes for fuldbyrdet overtrædelse af strfl. § 301 i sammenstød med forsøg på databedrageri efter strfl. § 279 a, jf. § 21[154]. I den sammenhæng fremhæves det, at der kun bør dømmes for forsøg på databedrageri i sammenstød med strfl. § 301, "hvor gerningsmanden enten har haft mislykkede forsøg på anvendelse eller er taget på fersk gerning i sit forsøg på at bruge de generede kort."[155] Dette skyldes, at den blotte besiddelse af hvide kort er strafbelagt i strfl. § 301.

Modsætningsvist mener Lasse Lund Madsen, at der ikke bør straffes i sammenstød ved strfl. § 301 og forsøg på databedrageri, jf. strfl. § 279 a, jf. § 21[156]. Dette begrunder han ved at henvise til baggrunden for indførelsen af strfl. § 301 og dens sammenhæng med forsøgsansvaret[157].

Som anført i afsnit 4.4.2 vil selve brugen af betalingskortoplysningerne ofte kunne henføres under strfl. §§ 279 eller 279 a. Det at skaffe sig oplysninger, vil derfor typisk udgøre forsøg på bedrageri eller databedrageri efter strfl. §§ 279 eller 279 a. Lasse Lund Madsen mener

[152] Betænkning nr. 1417/2002, pkt. 3.6.2
[153] Langsted, U.2019B.48, Dankortet i strafferetlig belysning, s. 4 og Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed s. 5
[154] U.2019B.48, s. 4
[155] Langsted, U.2019B.48, Dankortet i strafferetlig belysning, s. 4
[156] U.2106B.343, s. 5
[157] U.2016B.343, s. 5

imidlertid, at straf i sammenstød vil skabe usikkerhed fordi forsættet skal være konkretiseret i henhold til brugen af de pågældende anskaffede oplysninger ved forsøg efter strfl. § 279 a[158]. Han er af den opfattelse, at der kun skal straffes efter strfl. § 301 hvis der ikke ved f.eks. skimming er forsæt til konkret brug af de anskaffede koder[159]. Ifølge ham er det afgørende for grænsedragningen mellem strfl. §§ 301 og 279 a, at der ved strfl. § 301 "ses bort fra det normalt stillede krav om bevis for forsæt til en nærmere konkretiseret handling."[160] Hvis der omvendt er et konkretiseret forsæt til at anvende de anskaffede koder på den måde, som er anført i bestemmelsen om databedrageri, mener han, at der kun skal straffes for forsøg på databedrageri, såfremt der ikke sker fuldbyrdelse[161]. Dette skyldes, at skimming, som nævnt må anses for at være forstadiet til det efterfølgende databedrageri, og ved konkretiseret forsæt til databedrageri vil forsøgsansvaret være opfyldt.

Ved en analyse af retspraksis har det vist sig, at der siden indførelsen af strfl. § 301 ikke har været en konsekvent tilgang til bestemmelsens anvendelse i tiltalepraksis. Således blev der i dommen TfK 2011.388 Ø, udelukkende rejst tiltale og dømt for overtrædelse af strfl. § 279 a, jf. § 286, stk. 2 og forsøg herpå. Dommen omhandlede opsætning af skimmingudstyr til at indsamle oplysninger, der blev anvendt til at fremstille falske betalingskort, som derefter blev brugt til uberettigede hævninger og forsøg herpå. Anklagemyndigheden subsumerede hele forholdet under strfl. § 279 a og inddragede ikke den indledende skimming, der er omfattet af strfl. § 301. Denne dom anses ikke for at være udtryk for gældende retstilstand, da der i flere efterfølgende domme er blevet rejst tiltale efter både strfl. §§ 301 og 279 a, når begge bestemmelsers gerningsindhold fuldbyrdes[162].

Omvendt rejste anklagemyndigheden kun tiltale for overtrædelse af strfl. § 301 i dommen AM2013.03.18B, og subsumerede hele forholdet under denne bestemmelse. Sagen angik opsætning af skimmingudstyr på en tankstation, hvor der blev indsamlet oplysninger fra 72 betalingskort med forsæt til uberettiget brug af disse oplysninger. Der tages i dommen kun stilling til opsætningen af skimmingudstyret, som er omfattet af strfl. § 301. Det antages, at der kun blev rejst tiltale for § 301, da der i sagen ikke var konkret forsæt til at anvende de opnåede oplysninger til databedrageri. Dette understøttes af, at det i dommen ikke blev nævnt, at der

[158] U.2016B.343, s. 5
[159] Ibid. s. 5
[160] LFF 2003-11-05, nr. 55, alm. bem., pkt. 3.2.2
[161] U.2016B.343, s. 5
[162] Se f.eks. TfK 2015.590 V og TfK 2018.751 V

var forsæt til indgreb i elektronisk databehandling, hvorfor forholdet ikke var omfattet af bestemmelsen om databedrageri [163].

I dommen TfK 2018.751 V blev tiltalte dømt for fuldbyrdelse af strfl. § 301, ved at have "opsat skimmingsudstyr på betalingsautomater med forsæt til at aflure og kopiere betalingskortoplysninger". Tiltalte blev ligeledes dømt for forsøg på medvirken til databedrageri af særlig grov beskaffenhed. Det anføres i dommen, at "der [var] sket misbrug af betalingskort som følge af skimmingen ved hævning og forsøg på hævning". Da databedrageri omfatter misbrug af betalingskort, er det derved klargjort i dommen, at der har været konkret forsæt til at anvende betalingskortoplysningerne fra skimmingen på den måde, som er anført i strfl. § 279 a. Dommen viser, at der straffes for fuldbyrdelse af strfl. § 301 og forsøg på strfl. § 279 a. Strfl. § 301 absorberes dermed ikke under strfl. § 279 a ved konkret forsæt til anvendelse af de indsamlede oplysninger.

Ud fra den gennemgåede retspraksis kan det udledes, at hvis forsættet til anvendelsen af oplysninger omfattet af strfl. § 301 er konkretiseret, så straffes der både efter strfl. §§ 301 og 279 a. Hvis forsættet til uberettiget anvendelse derimod ikke er konkret straffes der kun efter strfl. § 301. Retspraksis understøtter derved Lars Bo Langsteds konklusion om, at der kan straffes både efter strfl. § 301 og forsøg på strfl. § 279 a, hvis forsæt til anvendelse er tilstrækkeligt konkret[164].

Vi mener, at dette er i overensstemmelse med bestemmelsernes anvendelsesområde. Baggrunden for dette er, at gerningsindholdet i strfl § 301 ikke omfatter anvendelsen af betalingskortoplysninger, men kun fremstilling, anskaffelse, besiddelse eller videregivelse. Selvom oplysningerne, der opnås ved skimming i de fleste tilfælde må antages at skulle anvendes til at begå databedrageri, vil subsumeringen af skimmingforholdet under strfl. § 279 a medføre en udvidelse af strfl. § 279 a og at der ses bort fra strfl. § 301. Dette harmonerer ikke med formålet med indførelsen af strfl. § 301, idet ideen var at gøre selve besiddelsen mv. af oplysninger strafbart[165].

[163] En lignende dom er U 2014.1241 V, hvor der ligeledes kun blev rejst tiltale efter strfl. § 301, og hvor forsættet til uberettiget anvendelse af kortoplysningerne heller ikke synes at være konkret.
[164] Se også dommene TfK 2015.590 V og TfK 2016.464 V, hvor der også dømmes for fuldbyrdet overtrædelse af strfl. § 301 og forsøg på strfl. § 279 a.
[165] Betænkning nr. 1417/2002, pkt. 4.3.3

Afgrænsningen har betydning for, at bestemmelserne bliver anvendt i overensstemmelse med deres tiltænkte formål, og at der derved dannes klare retningslinjer ved tiltalerejsning. Derudover skaber det et tydeligere billede af hele handlingsforløbet , når der straffes i sammenstød ved strfl. §§ 301 og 279 a, jf. § 21.

Kapitel 5 - Hemmelig ransagning

5.1 Samspillet mellem hemmelig ransagning, indgreb i meddelseshemmeligheden og dataaflæsning[166]

Indførelsen af strfl. § 279 a medførte materielle afgrænsningsproblemer, især i forhold til strfl. § 276, jf. ovenstående afsnit. Bestemmelsens indførelse har imidlertid også skabt processuelle udfordringer, da denne type kriminalitet foregår i den virtuelle verden. Spørgsmålet er derfor om politiets efterforskningsmuligheder efter retsplejeloven kan følge med den teknologiske udvikling. Dette spørgsmål vil blive behandlet i henhold til om reglerne omkring hemmelig ransagning, jf. rpl. § 799, er hensigtsmæssige, da der ikke er hjemmel til at foretage dette indgreb ved databedrageri.

Bestemmelserne om indgreb i meddelelseshemmeligheden og dataaflæsning vil også blive behandlet. Baggrunden for dette er, at der er visse grænsetilfælde mellem disse indgreb og hemmelig ransagning, hvor det kan være vanskeligt at vurdere, hvilket indgreb der finder anvendelse. Afgrænsning mellem indgrebene er vigtig, idet det har betydning for, om indgrebet finder anvendelse ved databedrageri efter strfl. § 279 a.

5.1.1 Ransagning - rpl. kapitel 73

Politiets mulighed for at foretage ransagning med henblik på at indsamle beviser, må anses for at være et vigtigt og centralt led i efterforskningen. Formålet med ransagning i forbindelse med databedrageri, jf. strfl. § 279 a, vil typisk være at beslaglægge varer, som er blevet købt ved misbrug af andre personers betalingskortoplysninger[167].

Ransagning må anses for at være et forholdsvis alvorligt tvangsindgreb, da der sker en krænkelse af husfreden og privatlivets fred, jf. GRL § 72 og EMRK art. 8. Det følger af

[166] Reglerne om kompetence, advokatbeskikkelse mv. vil ikke blive gennemgået for disse indgreb
[167] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 5

grundlovens § 72, at "Boligen er ukrænkelig. Husundersøgelse [og] beslaglæggelse (...) må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse." Det fremgår endvidere af EMRK art. 8, at "enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance", hvorefter der er mulighed for efter stk. 2, at foretage indgreb hvis der er hjemmel i national lov.

I dansk ret er der ifølge retsplejelovens kapitel 73 hjemmel til at foretage ransagning. Det følger af dette kapitel, hvad der er genstand for ransagning, samt hvilke betingelser der skal være opfyldt, før ransagning kan gennemføres.

Genstand for ransagning - rpl. § 793

Ved ransagning har politiet mulighed for at foretage undersøgelser af en persons "[bolig] og andre husrum, dokumenter, papirer og lignende samt indholdet af aflåste genstande", jf. rpl. § 793, stk. 1, nr 1 (kategori 1-ransagning). Derudover kan ransagning foretages af "andre genstande samt lokaliteter uden for husrum", jf. rpl. § 793, stk. 1, nr. 2 (kategori 2-ransagning).

Betingelserne for ransagning - rpl. §§ 794 og 795

Betingelserne for at foretage ransagning fremgår af rpl. §§ 794 og 795. Der sondres mellem, om det er en mistænkt som har rådighed over lokaliteten og genstandene, eller om de er under en ikke-mistænkts rådighed.

Rpl. § 794 omhandler betingelserne for at foretage ransagning hos en mistænkt. Efter bestemmelsen kan ransagning gennemføres, hvis den "pågældende med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og ransagning må antages at være af væsentlig betydning for efterforskningen", jf. rpl. § 794, stk. 1, nr. 1 og 2. Ved kategori 1-ransagninger kræves der yderligere, "at sagen angår en lovovertrædelse der efter loven kan medføre fængselsstraf, eller at der er bestemte grunde til at antage, at bevis i sagen eller genstande, der kan beslaglægges, kan findes ved ransagningen", jf. rpl. § 794, stk. 2. Herved sker der en skærpelse af henholdsvis kriminalitetskravet og indikationskravet, jf. rpl. § 793, stk. 1, nr. 1, jf. § 794 , stk. 2.

Betingelserne for at foretage ransagning hos ikke-mistænkt fremgår af rpl. § 795. Efter bestemmelsen finder reglerne i rpl. kapitel 73 ikke anvendelse ved skriftlig samtykke til ransagning, fra den som indgrebet angår, eller hvis pågældende giver samtykke i tilslutning til opdagelse af en forbrydelse. Hvis der ikke gives samtykke til at foretage ransagning kræves det, at "efterforskning vedrører en lovovertrædelse, der efter loven kan medføre fængselsstraf", jf. rpl. § 795, stk. 1, nr. 1. Derudover kræves det, at "der er bestemte grunde til at antage, at

bevis i sagen eller genstande, der kan beslaglægges, kan findes ved ransagning", jf. rpl. § 795, stk. 1, nr. 2. Det følger af bestemmelsens forarbejder, at indikationskravet efter rpl. § 795, stk. 1, nr. 2 skal forstås noget strengere end kravet ved ransagning hos en mistænkt[168].

Der er mulighed for at foretage ransagning ved databedrageri efter strfl. § 279 a, idet kriminalitetskravet hverken ved ransagning hos mistænkt eller ikke-mistænkt er særligt strengt.

Fremgangsmåde - rpl. § 798

Det følger af rpl. § 798, stk. 2, at vedkommende som har rådighed over genstanden for ransagning skal "gøres bekendt med ransagningens foretagelse og grundlaget herfor samt opfordres til at overvære ransagningen." Hvis den pågældende er fraværende men der er andre tilstedeværende, skal disse gøres bekendt med ransagning og opfordres til at overvære den, jf. rpl. § 798, stk. 2. Hvis de tilstedeværende forsøger at hindre ransagningens gennemførelse, kan politiet fjerne dem mens ransagningen gennemføres, hvis øjemed gør det påkrævet, jf. rpl. § 798, stk. 2.

Personen som har rådighed over genstanden for ransagning kan som udgangspunkt kræve, at et vidne som vedkommende har udpeget er til stede ved ransagningen, jf. rpl. § 798, stk. 2. Udgangspunktet kan fraviges, hvis der er tidsmæssige eller efterforskningsmæssige grunde der taler for det f.eks. ved mistanke om at vidnet er medskyldig.

Foretages der kategori 1-ransagning, hvor der ikke er nogen tilstedeværende, skal politiet bestræbe sig på, at tilkalde to husfæller eller andre vidner der kan overvære ransagningen, jf. rpl. § 798, stk. 3. Efter kategori 1-ransagning er afsluttet, skal pågældende der har rådighed over genstanden for ransagning underrettes, jf. rpl. § 798, stk. 1.

5.1.2 Hemmelig ransagning - rpl. § 799

Hemmelig ransagning betyder, at der under visse betingelser kan foretages ransagning uden at mistænkte eller andre, herunder vidner, gøres bekendt med indgrebet, jf. rpl. § 799, stk. 1. Dette har især stor betydning af hensyn til at "undgå, at den fremtidige efterforskning vanskeliggøres eller umuliggøres derved, at de implicerede og navnlig bagmænd advares."[169]

[168] Betænkning nr. 1159/1989, alm. bem., pkt. 4.1.2
[169] Betænkning 1159/1989, alm. bem., pkt. 5.5.

Betingelser for hemmelig ransagning

Ifølge rpl. § 799, stk. 1, kan indgrebet kun foretages "såfremt det er af afgørende betydning for efterforskningen". Indikationskravet er derved skærpet ved hemmelig ransagning i forhold til ved almindelig ransagning.

Kriminalitetskravet i bestemmelsen er også skærpet i forhold til ved almindelig ransagning, eftersom indgrebet kun kan ske, "hvis efterforskningen angår en forsætlig overtrædelse" af en række nærmere angivne alvorlige straffelovsovertrædelser, jf. rpl. § 799, stk. 1. Da strfl. §§ 279 a eller 286, stk. 2, ikke indgår i opregningen af straffelovsbestemmelser i rpl. § 799, stk. 1, kan hemmelig ransagning ikke foretages ved databedrageri.
Hvis der forud for databedrageri er begået tyveri af grov beskaffenhed efter strfl. § 286, stk. 1, jf. § 276, kan hemmelig ransagning dog foretages på baggrund af dette forhold, jf. rpl. § 799, stk. 1.

Mistankekravet er ikke skærpet, og må antages at følge rpl. § 794, stk. 1, nr. 1[170], hvorefter en person "med rimelig grund [skal være] mistænkt for en lovovertrædelse, der er undergivet offentlig påtale". Hemmelig ransagning kan ligesom ved almindelig ransagning, også foretages over for en ikke-mistænkt[171].

Kompetence

Afgørelse om indgrebet træffes af retten ved kendelse, jf. rpl. § 799, stk. 1. I den forbindelse træffer retten ligeledes afgørelse om, at "reglerne i § 798, stk. 2, 1.-4. pkt. og stk. 3, fraviges", jf. rpl. § 799, stk. 1,. Rpl. § 798 omhandler bl.a. vidners overværelse af ransagning, og hvis bestemmelsen ikke kunne fraviges, ville formålet med hemmelig ransagning være svært at gennemskue.

Rpl. § 799, stk. 2 henviser til udvalgte bestemmelser om indgreb i meddelelseshemmeligheden, som finder anvendelse ved hemmelig ransagning[172]. Der er bl.a. tale om reglerne omkring

[170] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 5, fodnote 14
[171] Kistrup m.fl., Straffeprocessen, 2018, s. 489
[172] Der henvises til afsnittet om indgreb i meddelelseshemmeligheden

tidsfrist ved indgreb, jf. rpl. § 783, stk. 3 og 4, og reglerne om efterfølgende underretning, når indgreb er afsluttet, jf. § 788[173].

Gentagne hemmelige ransagninger

Rpl. § 799, stk. 3[174], giver politiet hjemmel til at foretage flere gentagne hemmelige ransagninger inden for en periode på 4 uger. Dette følger af, at retten kan bestemme, at der kan foretages gentagne hemmelige ransagninger inden for det tidsrum der fastsættes efter rpl. § 799, stk. 2, jf. § 783, stk. 3[175].

Udgangspunktet er, at "retten skal (...) fastsætte antallet af ransagninger", jf. § 799, stk. 3. Retten har imidlertid mulighed for at bestemme, at der kan "foretages et ubestemt antal ransagninger" inden for det fastsatte tidsrum, "hvis særlige grunde taler derfor", jf. § 799, stk. 3.

5.1.3 Indgreb i meddelelseshemmeligheden - rpl. kapitel 71

Indgreb i meddelelseshemmeligheden kan være et effektivt indgreb og have stor efterforskningsmæssig betydning i sager, hvor det kan være vanskeligt at skaffe beviser på anden måde[176]. Over for hensynet til efterforskningen står imidlertid hensynet til individets rettigheder. Således skal grundlovens § 72 og EMRK art. 8, ligesom ved ransagning, iagttages. Efter grundlovens § 72 kræver "undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden" retskendelse, med mindre andet er hjemlet ved lov. I dansk ret er der hjemmel til at foretage indgreb i meddelelseshemmeligheden efter retsplejeloven kap. 71, hvor de forskellige betingelser og specielle hensyn i forbindelse med indgrebet er fastlagt.

[173] Derudover angår det reglerne om indgrebsadvokat og dennes aktindsigt jf. rpl. §§ 784 og 785, hvilket ikke vil blive behandlet nærmere

[174] Bestemmelsens stk. 3 blev bl.a. indført som en følge af kendelsen U 1999.985 H, jf. LFF 2001-12-13 nr. 35, alm. bem., pkt. 3.3.2.2. Sagen omhandlede overtrædelse af strfl. § 191. Politiet havde i forbindelse med efterforskningen anmodet retten om tilladelse til, at foretage "flere enkeltstående hemmelige ransagninger [efter rpl. § 799] på en nærmere angivet adresse" inden for den tidsfrist, som retten havde fastsat. "Der fandtes imidlertid ikke i ordlyden af § 799 og bestemmelsens forarbejder at være tilstrækkelig klar hjemmel til, at en kendelse om tilladelse til ransagning efter § 799 kan udstrækkes til at omfatte mere end én ransagning inden for den i kendelsen anførte periode."

[175] Rpl § 799, stk. 2 henviser til rpl. § 783, stk. 3, der omhandler regler omkring tidsfrist ved indgreb i meddelelseshemmeligheden

[176] Betænkning nr. 1023/1984, alm. bem., pkt. 2.1

De enkelte indgreb - rpl. § 780

Rpl § 780, stk. 1, opregner seks forskellige former for indgreb, som er omfattet af indgreb i meddelelseshemmeligheden. I det følgende vil de indgreb, der er mest relevante i forbindelse med databedrageri blive gennemgået.

Politiet kan foretage indgreb i meddelelseshemmeligheden "ved at aflytte telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning)", jf. rpl. § 780, stk. 1, nr. 1. Anden tilsvarende telekommunikation sidestilles med telefonsamtaler, og omfatter herved "al fjernkommunikation af information (med undtagelse af radiokommunikation (...)), der befordres ved hjælp af elektroniske bølger eller lignende overførelsesmedier, således, at meddelelsen er fremme hos modtageren praktisk taget samtidig med afsendelsen"[177]. Anden tilsvarende telekommunikation indbefatter derved mange forhold og også indgående e-mails vil være omfattet, jf. U 1999.178 V[178]. Der vil ligeledes kunne foretages indgreb ved aflytning af kommunikation der foregår over kommunikationsplatform[179] på internettet, når "meddelelserne er synlige for modtageren, og dermed »fremme« hos pågældende, samtidig med afsendelsen."[180]

Efter rpl. § 780, stk. 1, nr. 5 kan politiet ved indgreb i meddelelseshemmeligheden også "tilbageholde, åbne og gøre sig bekendt med indholdet af breve, telegrammer og andre forsendelser (brevåbning)". Bestemmelsen finder både anvendelse ved forsendelser og andre post-relaterede tilfælde, f.eks. ved postbokse[181].

Ved brevåbning åbner politiet forsendelsen og gør sig bekendt med indholdet, for derefter at lukke og videresende forsendelsen[182]. Modtageren eller afsenderen underrettes ikke forud for brevåbningen[183].

Hvis forsendelsen ønskes standset, kan politiet "standse den videre befordring af [forsendelsen] som nævnt i nr. 5 (brevstandsning)", jf. rpl. § 780, stk. 1, nr. 6. Dette kræver, at

[177] Betænkning nr. 1023/1984, alm. bem., pkt. 2.6.2.1
[178] "Antaget, at indgående e-mail må sidestilles med »anden tilsvarende telekommunikation« i retsplejelovens § 780, stk. 1, nr. 1."
[179] F.eks. Messenger
[180] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 8
[181] Kommenteret retsplejelov, 2018, s. 287
[182] Ibid. s. 287
[183] Ibid. s. 287

politiet indsender begæring til retten inden for 48 timer efter tilbageholdelsens iværksættelse, da der ellers skal ske viderebefordring, jf. rpl. § 790.

Materielle betingelser for indgrebene - rpl. § 781

De materielle betingelser for indgreb i meddelelseshemmeligheden fremgår af rpl. § 781, stk. 1. Mistankekravet medfører, at "indgreb i meddelelseshemmeligheden [kun må] foretages, såfremt der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt", jf. rpl. § 781, stk. 1, nr. 1. Det følger heraf, at mistanken skal være "rimelig og konkret"[184], jf. "bestemte grunde".

Ifølge indikationskravet, må indgrebet kun gennemføres når det "må antages at være af afgørende betydning for efterforskningen", jf. rpl. § 781, stk. 1, nr. 2. Indikationskravet er derved strengt, men det medfører ikke, at indgrebet kun kan foretages, hvis det er den sidste udvej og andre indgreb ikke lader sig gennemføre[185]. Indgreb i meddelelseshemmeligheden vil således også kunne ske, hvis andre indgreb vil medføre store ressourcemæssige konsekvenser. Dette kan f.eks. være tilfældet ved langvarig skygning af flere personer, el. hvis den igangværende efterforskning vil blive afsløret ved andre indgreb, f.eks. ransagning, hvor det risikeres at medgerningsmænd kan blive advaret[186].

Indgreb i meddelelseshemmeligheden kan kun foretages, såfremt "efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, [eller] en forsætlig overtrædelse af af straffelovens kapitler 12 eller 13", jf. rpl. § 781, stk. 1, nr. 3. Derudover kan der ske indgreb ved overtrædelse af visse nærmere opregnede straffelovsbestemmelser, som ikke har en strafferamme på fængsel i 6 år eller derover, jf. rpl. § 781, stk. 1, nr. 3. Kriminalitetskravet er derved strengt. Dette har betydning i henhold til muligheden for at foretage indgreb i forbindelse med databedrageri. Strfl. § 279 a indgår ikke som en af de oplistede straffelovsbestemmelser, der hjemler indgreb i meddelelseshemmeligheden. Konsekvensen af dette er, at kriminalitetskravet efter rpl. § 781, stk. 1, nr. 3, kun vil være opfyldt ved databedrageri af grov beskaffenhed, jf. strfl. § 286, stk. 2, jf. § 279 a. Indgreb i forbindelse med efterforskning af databedrageri vil derfor ikke kunne

[184] Kistrup m.fl., Straffeprocessen, 2018, s. 457
[185] Ibid. s. 459
[186] Ibid. s. 459

foretages med mindre forholdet er af "særligt grov beskaffenhed", jf. strfl. § 286, stk. 2, og "straffen [derved] kan stige til fængsel indtil 8 år".

Brevåbning og brevstandsning kan ske efter de almindelige mistanke-, indikations og kriminalitetskrav i rpl. § 781, stk. 1, nr. 1-3. Derudover kan indgrebene foretages efter den specielle bestemmelse i rpl. § 781, stk. 4, hvis "der foreligger en særligt bestyrket mistanke om, at der i forsendelsen findes genstande, som bør konfiskeres, eller som ved en forbrydelse er fravendt nogen, som kan kræve dem tilbage." Mistankekravet er derved skærpet. Den særlige mulighed for brevåbning og brevstandsning der fremgår af rpl. § 781, stk. 4, beror på en forudsætning om, at der "ved breve, pakker eller andre forsendelser (...) undertiden [sker] transport af genstande, der har en særlig tilknytning til et strafbart forhold, og som der ikke er nogen grund til at beskytte mod politiets indgreb."[187] Ved brevåbning og brevstandsning efter rpl. § 781, stk. 4, skal betingelserne i rpl. § 781, stk. 1, nr. 2 og 3, ikke være opfyldt. Dette betyder, at det strenge kriminalitetskrav ikke finder anvendelse. Derfor kan indgrebet foretages ved almindelig databedrageri.

Tidsfrist for indgrebet - rpl. § 783

Proportionalitetsprincippet i rpl. § 782, stk. 1 skal altid iagttages ved indgreb i meddelelseshemmeligheden. Det betyder, at indgreb ikke må "foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb", jf. rpl. § 782, stk. 1. På baggrund af dette følger det af rpl. § 783, stk. 3, at tidsrummet for indgrebet skal være angivet i rettens kendelse[188], og at tidsrummet skal være "så kort som muligt og [ikke må] overstige 4 uger". Forlængelse kan ske, men kun for 4 uger af gangen, og kun ved kendelse, jf. rpl. § 783, stk. 3. Dette er med til at sikre, at indgrebet ikke bliver mere byrdefuldt end sagens alvor tilsiger.

Bistand til indgrebet - rpl. § 786

Postvirksomhed og teleudbydere skal yde bistand til at politiet kan foretage indgreb i meddelelseshemmeligheden, jf. rpl. § 786, stk. 1. Denne bistand består i at "etablere aflytning

[187] Betænkning nr. 1023/1984, alm. bem., pkt. 2.6.5.1
[188] Det følger af rpl. § 783, stk. 1, at retten ved kendelse, som udgangspunkt træffer afgørelse om indgreb i meddelelseshemmeligheden

af telefonsamtaler mv., (...) samt (...) tilbageholde og udlevere forsendelser mv." til politiet, jf. rpl. § 786, stk. 1.

Underretning - rpl. § 788

Underretning om indgreb i meddelelseshemmeligheden gives først efter, at indgrebet er afsluttet, jf. rpl. § 788, stk. 1. Indtil da vil indgrebet være hemmeligt.

Underretningspligten kan i visse tilfælde fraviges. Hvis underretning vil være til skade for efterforskning af "anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, eller (...) hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller omstændighederne i øvrigt [taler] imod underretning" kan underretning således undlades eller udsættes, jf. rpl. § 788, stk. 4.

5.1.4 Dataaflæsning - rpl. § 791 b

Rpl. § 791 b blev indsat i 2002[189]. Før bestemmelsen om dataaflæsning havde politiet mulighed for ved det eksisterende indgreb i form af "aflytning [, jf. rpl. § 780, stk. 1, nr. 1, at] gøre sig bekendt med kommunikation mellem computere, ligesom politiet ved (...) ransagning [kunne] gøre sig bekendt med alle registreringer i en computer"[190]. Imidlertid var det ikke altid muligt for politiet at benytte de eksisterende indgreb "til at gøre sig bekendt med elektroniske meddelelser og materiale i en computer"[191], som følge af af tekniske udfordringer og risikoen for at blive afsløret. Dette var grundlaget for at bestemmelsen om dataaflæsning blev indført

Oplysninger og fremgangsmåde

Rpl. § 791 b hjemler adgang for politiet til at foretage "aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem[192] ved hjælp af [enten] programmer eller andet udstyr"[193].

[189] Ved lov nr. 378 af 6. juni
[190] LFF 2001-12-13 nr. 35, alm. bem., pkt. 1.2
[191] Ibid. alm. bem, pkt. 1.2
[192] Informationssystem skal forstås som "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 af bestemmelsen, hvis udstyret har funktioner svarende til dem, der findes i personlige computere", jf. LFF 2001-12-13, nr. 35, de specielle bemærkninger til rpl. § 791 b
[193] Dataaflæsning ved hjælp af enten programmer eller andet udstyr "kan ske ved hjælp af (teknisk) udstyr, der fysisk installeres i computeren, eller, i det omfang dette er teknisk muligt, ved at edb-

Heri ligger en implicit adgang for politiet til at skaffe sig adgang til computeren og "installere det tekniske udstyr, der skal anvendes ved indgrebet"[194].

Dataaflæsning kan foretages "ved hjælp af et såkaldt »sniffer-program« , [hvor politiet] får tilsendt kopi af samtlige indtastninger, som [den mistænkte] foretager, [i forbindelse med] åbning af computeren, oprettelse af nye dokumenter og regnskaber mv. og nye indtastninger i allerede eksisterende dokumenter"[195]. Indgrebet omfatter også det oplysninger som den mistænkte har modtaget og som er blevet lagret i computerens hukommelse[196].

Betingelser for indgrebet

Betingelserne for at foretage dataaflæsning fremgår af rpl. § 791 b, stk. 1. Mistankekravet medfører, at dataaflæsning kan foretages, såfremt der er "bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet (...)", jf. rpl. § 791 b, stk. 1, nr. 1. Derudover følger det af indikationskravet, at indgrebet kun kan gennemføres, hvis det "må antages at være af afgørende betydning for efterforskningen", jf. rpl. § 791 b, stk. 1, nr. 2. Efter kriminalitetskravet skal "efterforskningen [angå] en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13", jf. rpl. § 791 b, stk. 1, nr. 3.

Tidsfrist

Rpl § 791 b, stk. 3 henviser til reglerne om indgreb i meddelelseshemmeligheden. Det følger heraf, at der i kendelsen om dataaflæsning skal fastsættes et tidsrum som indgrebet kan foretages inden for, jf. rpl. § 791 b, stk. 3, jf. 783, stk. 3. Der henvises til afsnittet om indgreb i meddelelseshemmeligheden.

Underretning

Ved dataaflæsning skal der efter indgrebets afslutning ske underretning, jf. rpl. § 791 b, stk. 4. Rpl. § 788, stk. 1, 3 og 4, finder anvendelse ved underretning, jf. rpl. § 791 b, stk 4. Der henvises til afsnittet om indgreb i meddelelseshemmeligheden.

---

programmer eller lignende sendes til den pågældende computer", jf. LFF 2001-12-13, nr. 35, de specielle bemærkninger til rpl. § 791 b

[194] LFF 2001-12-13 nr. 35, de specielle bemærkninger til rpl. § 791 b

[195] Ibid. de specielle bemærkninger til rpl. § 791 b

[196] Ibid. de specielle bemærkninger til rpl. § 791 b

5.1.5 Afgrænsningen mellem de forskellige tvangsindgreb

Grunden til, at afgrænsningen mellem indgrebene har betydning er dels, at der er forskel på de krav der skal opfyldes for at indgreb kan foretages, dels at der består en forskel i, hvorvidt indgrebet kan hemmeligholdes over for den som indgrebet angår[197]. Derudover kan det være vigtigt at anvende flere forskellige tvangsindgreb under efterforskningen, for at kunne indsamle beviser for hele det kriminelle forløb. Dertil kommer, at det i visse tilfælde kan være umuligt at anvende et indgreb, selvom betingelserne for at foretage indgrebet er opfyldt - derfor kan det være nødvendigt med en mulighed for et alternativt indgreb. Ved databedrageri kan dette imidlertid være problematisk, eftersom hemmelig ransagning ikke finder anvendelse.

Indgreb i meddelelseshemmeligheden og ransagning

Afgrænsningen mellem indgreb i meddelelseshemmeligheden og ransagning er især vigtig fsva. brevåbning og brevstandsning i forhold til ransagning. Misbrug af betalingskort til køb af varer på internettet er en typisk form for databedrageri. I denne forbindelse er det vigtigt for politiet at standse forsendelsen, og derved forhindre udlevering af genstande fra det strafbare forhold.

Rpl. § 780 om indgreb i meddelelseshemmeligheden, finder kun anvendelse ved meddelelser undervejs i en "kommunikationslinje mellem to eller flere personer."[198] Hvis indgreb foretages inden eller efter kommunikation er påbegyndt el. afsluttet, vil det være reglerne om enten edition eller ransagning og beslaglæggelse der finder anvendelse[199]. Således vil tilfælde, hvor et brev enten ikke er blevet sendt endnu, el. det er kommet frem til modtageren og åbnet, være omfattet af reglerne om ransagning og beslaglæggelse[200]. Det samme gælder ved sms'er der er modtaget og lagret, jf. U 2008.1734 V[201].

Hvis modtageren af et brev har en postboks på posthuset, hvor brevet er lagt i, og politiet med postvæsenets bistand ønsker at gøre sig bekendt med brevets indhold uden, at modtageren underrettes herom, er det reglerne om indgreb i meddelelseshemmeligheden der finder

[197] Kistrup m.fl., Straffeprocessen, 2018, s. 452, og betænkning nr. 1023/1984, alm. bem., pkt. 2.6.2
[198] Kistrup m.fl., Straffeprocessen, 2018, s. 451
[199] Reglerne om edition og beslaglæggelse vil ikke blive behandlet nærmere.
[200] Kistrup m.fl. Straffeprocessen, 2018, s. 451
[201] "Spørgsmålet om politiets adgang til - uden bistand fra vedkommende teleselskab - at gøre sig bekendt med indholdet af sms-beskeder, der er modtaget og lagret i en mobiltelefon, skal afgøres efter retsplejelovens regler om ransagning og beslaglæggelse, idet sådanne sms-beskeder må sidestilles med breve, der er kommet frem til adressaten."

anvendelse[202]. Dette skyldes, at brevet stadig anses for at være undervejs i en kommunikationslinje. Har politiet derimod en nøgle til postboksen, så de dermed selv kan åbne denne, vil det omvendt være reglerne om ransagning der skal benyttes[203]. "Elektronisk post, der beror hos en Internetudbyder, må sidestilles med breve i en postboks"[204]. Hvis eksemplet med postboksen skal overføres til internettet vil dette betyde, at i tilfælde, hvor politiet er i besiddelse af adgangskoden til en elektronisk boks, og derved kan logge ind uden bistand fra internetudbyder, vil det være reglerne om ransagning der finder anvendelse[205]. Modsat er det reglerne om indgreb i meddelelseshemmeligheden der skal anvendes, hvor internetudbyderens bistand er påkrævet for, at politiet kan foretage indgrebet. Afgørende for afgrænsningen er derfor, om bistand er påkrævet eller ej.

Indgreb i meddelelseshemmeligheden, dataaflæsning og hemmelig ransagning

På grund af de mange muligheder kriminelle har fået for at kommunikere på internettet, er det vigtigt at politiet har mulighed for at foretage forskellige indgreb i denne kommunikation. I den forbindelse er det relevant at behandle indgreb i meddelelseshemmeligheden, dataaflæsning og hemmelig ransagning, da disse indgreb gør det muligt for politiet at følge med i denne kommunikation.

Afgrænsningen mellem dataaflæsning og hemmelig ransagning skal findes i U 2012.2614 H[206]. I sagen havde politiet fået adgang til tiltaltes Facebook- og Messengerprofiler, dvs. en kommunikationsplatform[207], med rette koder, som var indsamlet ved telefonaflytning. I den forbindelse loggede politiet ind på Facebookprofilen "med henblik på at konstatere, om der fortsat var adgang til profilen." By og landsretten tillod de foretagne og fremadrettede indgreb efter rpl. § 791 b om dataaflæsning. Højesteret kom imidlertid frem til den konklusion, at "politiets adgang til T's Facebook- og Messengerprofiler ved brug af koderne var indgreb, som

[202] Kistrup m.fl. Straffeprocessen, 2018, s. 452
[203] Ibid. s. 452
[204] jf. betænkning 1377/1999, pkt. 7.4. Se også U 1998.1613 Ø: "Politiet ønskede, at det skulle pålægges tredjemand at udlevere de e-mail, som var placeret på sigtedes kontoangivelser. Denne post måtte sidestilles med post, som var kommet frem til sigtedes bopæl."
[205] Betænkning 1377/1999, pkt. 6.1
[206] Sagen angik efterforskning af narkotikakriminalitet efter strfl. § 191
[207] "En kommunikationsplatform på internettet [skal forstås som et privat chatforum, f.eks. Facebook eller Messenger] hvor én eller flere personer privat kan udveksle oplysninger, således at hver bruger har oprettet en profil med password", jf. Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 3, fodnote 2

havde karakter af gentagne hemmelige ransagninger, som kan foretages med hjemmel i retsplejelovens § 793, stk. 1, nr. 1, jf. § 799."

Anklagemyndigheden havde for Højesteret påstået indgrebene henført under rpl. § 799, subsidiært rpl. § 791 b. Højesteret tog ikke stilling til, hvorvidt indgrebene kunne have været omfattet af den subsidiære påstand om dataaflæsning, men henførte blot forholdet under rpl. § 799. Anklagemyndigheden anførte imidlertid i deres anbringender, at "efter forarbejderne til retsplejelovens § 791 b, stk. 1, synes reglerne om dataaflæsning navnlig at være rettet mod tilfælde, hvor politiet ved at installere snifferprogrammer eller andet udstyr i f.eks. en computer kan skaffe sig adgang til oplysninger i denne."[208] Da aflæsning af oplysningen ikke skete ved brug af programmer eller andet udstyr, mente anklagemyndigheden, at forholdet ikke var omfattet af reglerne om dataaflæsning. Ud fra anklagemyndighedens argumentation er det afgørende for afgrænsningen, om adgangen til kommunikationsplatformen sker ved hjælp af programmer eller andet udstyr, eller om adgangen sker uden brug af teknisk udstyr.

Angående muligheden for at henføre indgrebet under reglerne om indgreb i meddelelseshemmeligheden anførte Højesteret, at de oplysninger som politiet fik kendskab til ved indgrebene, ikke var undervejs i en kommunikationslinje, og derfor kunne sammenlignes med afsendte og modtagne e-mails[209]. Højesteret konkluderede at når "oplysningerne [var] lagret på profilerne og tilgængelige ved hjælp af koderne"[210] var det reglerne om gentagne hemmelige ransagninger der fandt anvendelse.

Grundlæggende for afgrænsningen af hvilket indgreb der finder anvendelse er, måden som politiet får adgang til kommunikationsplatformen på.

"Først når bistand fra internetudbyderen eller et telefonselskab er fornøden, finder reglerne om indgreb i meddelelseshemmeligheden anvendelse."[211] Dette skyldes, at når politiet selv kan logge på en kommunikationsplatform med rette koder, anses kommunikationen ikke længere for at være undervejs i en kommunikationslinje.

[208] U 2012.2614 H
[209] U 2012.2614 H
[210] U 2012.2614 H
[211] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 10

"Når indgrebet på kommunikationsplatform [foretages] ved, at politiet installerer programmer eller udstyr i den mistænktes computer, er der tale om dataaflæsning."[212] I de situationer hvor politiet kontinuerligt logger på en kommunikationsplatform med rette koder vil dette være omfattet af reglerne om gentagne hemmelige ransagninger, jf. rpl. § 799, stk. 3.

De oplysninger som politiet får kendskab til i forbindelse med indgrebene kan være det samme, men afgrænsningen er især relevant ved databedrageri af grov beskaffenhed, jf. strfl. § 286, stk. 2, jf. § 279 a, da der ikke er hjemmel til at foretage hemmelig ransagning ved denne kriminalitetstype.

Er bestemmelsen om hemmelig ransagning mere indgribende end indgreb i meddelelseshemmeligheden og dataaflæsning?

Ud fra afgrænsningen mellem de forskellige indgreb kan det fastslås, at der er grænsetilfælde, hvor bestemmelsernes overlapper hinanden. Derfor kan det virke bemærkelsesværdigt, at hemmelig ransagning har et mere snævert anvendelsesområde end de andre indgreb. Spørgsmålet er, om dette kan begrundes ud fra indgrebets intensitet.

Lene Wacher Lentz argumenterer for, at hemmelig ransagning på kommunikationsplatforme faktisk kan være det mindst indgribende af de tre indgreb. Således anfører hun, at politiet ved indgreb i meddelelseshemmeligheden, hvor telefoner og e-mails mv. aflyttes, får kendskab til "alle samtaler og meddelelser, uanset indhold, til og fra den pågældende telefon eller e-mailadresse mv."[213] Endvidere vil politiet ved dataaflæsning få kendskab til "al aktivitet på en konkret computer, inklusiv meddelelser til og fra computeren samt færden på internettet."[214] Ved hemmelig ransagning retter politiets indgreb sig kun mod en specifik kommunikationsplatform, der er nærmere angivet[215]. Indgrebene kan resultere i, at politiet får indsamlet de samme efterforskningsmæssigt relevante oplysninger. Imidlertid omfatter indgreb i meddelelseshemmeligheden og dataaflæsning en større informationsstrøm, da disse indgreb også kan indeholde informationer der er efterforskningen uvedkommende.

[212] Wacher Lentz, Juristen nr. 1 2016, Hemmelig ransagning og brevstandsning i den digitale virkelighed, s. 10
[213] Ibid. s. 10
[214] Ibid. s. 10
[215] Ibid. s. 10

Der kan argumenteres for, at muligheden for at foretage hemmelig ransagning ved fysiske husrum taler for at indgrebet er mere intensivt. Dette skyldes at mange nok anser indgrebet som en betydelig krænkelse af boligens ukrænkelighed efter grl. § 72. Boligens ukrænkelighed udgør et vigtigt grundlag for retten til privatliv, da det er individets absolutte fristed, hvor vedkommende kan være sig selv uden indblanding udefra. Når det tages i betragtning, at hemmelig ransagning foretages uden mulighed for, at overvære indgrebet, vil indgrebet muligvis virke meget intensivt for den berørte. Dette synspunkt understøttes af Eva Smith der anfører, at " hemmelige ransagninger er et voldsomt middel. Borgerne i et demokratisk samfund må kunne stole på, at politiet ikke bryder hemmeligt ind i ens hjem, gennemsøger tingene og går igen uden at efterlade spor (...). Det er en metode, som bringer tankerne hen på samfund, som vi normalt ikke sammenligner os med."[216]

Grundlæggende er vi af den opfattelse, at hvis hemmelig ransagning foretages på en elektronisk kommunikationsplatform må det anses for at være mindre indgribende end indgreb i meddelelseshemmeligheden og dataaflæsning. Hvis indgrebet derimod retter sig mod husrum må det anses for mere intensivt end de andre indgreb, da dette indgreb i privatsfæren kan virke mere krænkende.

5.2 Formålet med indførelsen af rpl. § 799

I dette afsnit vil formålet med indførelsen af rpl. § 799 blive behandlet. Baggrunden for dette er, at vi ønsker at undersøge, om der i forarbejderne til rpl. § 799 kan findes en forklaring på, hvorfor bestemmelsen ikke finder anvendelse ved databedrageri.

1997

Rpl. § 799 blev indført i 1997[217]. Efterfølgende er bestemmelsen blevet udvidet op til flere gange på baggrund af, hvad der har været en samfundsmæssig problematik på det pågældende tidspunkt[218]. Oprindeligt skal indførelsen af rpl. § 799 ses i lyset af behovet for at kunne foretage indgrebet ved grov narkotikakriminalitet, og pga. den store nordiske rockerkrig der udspillede sig i 90'erne[219]. Hemmelig ransagning ved denne type kriminalitet kan være af stor

[216] https://www.berlingske.dk/samfund/politiet-faar-friere-haender-til-hemmelig-ransagning, (tilgået d. 16/5-19)
[217] Ved Lov nr. 411 af 10. juni 1997
[218] Ændret ved lov nr. 378 af 6. juni 2002 og lov nr. 634 af 12. juni 2013. Bestemmelsen blev også ændret i 2006, 2010 og 2017, men disse ændringer bliver ikke behandlet i specialet.
[219] LFF 1996-11-28 nr. 98, alm. bem., pkt. 5.4.2 og LFF 2013-02-28 nr. 164, alm. bem., pkt. 5.1

efterforskningsmæssig betydning, idet risikoen for "at den fremtidige efterforskning vanskeliggøres eller umuliggøres [og] at de implicerede og navnlig bagmænd advares"[220] derved minimeres. Heraf kan udledes, at indgrebet primært anses for nødvendigt ved "kriminalitet, der begås af en flerhed af personer"[221], hvor det skal være "muligt at hemmeligholde den igangværende efterforskning"[222]. Oprindelig var bestemmelsen om hemmelig ransagning tiltænkt kun at skulle finde anvendelse ved denne type kriminalitet, og indgrebet skulle kun ske "i absolutte undtagelsestilfælde"[223].

2002

Den første ændring til bestemmelsen fandt sted i 2002[224]. Ændringen medførte en udvidelse af indgrebets kriminalitetskrav, hvorvefter bestemmelsen kom til at omfatte andre alvorlige forbrydelser. Endvidere blev muligheden for, at politiet kunne foretage gentagne hemmelige ransagninger tilføjet som stk. 3 i bestemmelsen. Baggrunden for ændringen var det forhøjede trusselsniveau efter terrorangrebet d. 11. september 2001, der ifølge Justitsministeren gjorde det nødvendigt at udvide politiets adgang til at foretage hemmelige ransagninger. De samme hensyn gjorde sig gældende ved udvidelsen af kriminalitetskravet, som da bestemmelsen blev indført, nemlig at hemmelig ransagning kan være "afgørende for ikke at afsløre en igangværende efterforskning"[225].

Behovet for at kunne foretage gentagne hemmelige ransagninger bliver i forarbejderne begrundet ud fra flere synspunkter[226]. For det første er der behov for at kunne foretage gentagne hemmelige ransagninger i tilfælde, hvor politiet ikke finder beviser ved første ransagning, men der er mistanke om, at beviser kan findes inden for et kort tidsrum på stedet for ransagningen[227]. Dernæst kan behovet opstå i de situationer, hvor politiet ikke har haft mulighed for at foretage en nærmere undersøgelse af dokumenter eller lignende da ransagningen, på grund af risiko for at blive afsløret, bliver foretaget under tidspres[228]. Grundlæggende er gentagne hemmelige

[220] LFF 1996-11-28 nr 98, alm. bem., pkt. 5.3.6
[221] Ibid. alm. bem., pkt. 5.4.2
[222] Ibid. alm. bem., pkt. 5.4.2
[223] Betænkning nr. 1159/1989, alm. bem., pkt. 5.5
[224] Ved lov nr. 378, 6. juni 2002
[225] LFF 2001-12-13 nr. 35, alm. bem., pkt. 3.3.2.1
[226] Ibid. alm. bem., pkt. 3.3.2.2
[227] Fokus var især på narkotikakriminalitet og våbenlovsovertrædelser, jf. LFF 2001-12-13 nr. 35, alm. bem., pkt. 3.3.2.2
[228] LFF 2001-12-13 nr. 35, alm. bem., pkt. 3.3.2.2

ransagninger derved nødvendigt for, at politiet ikke forspilder muligheden for at retsforfølge, da de ved indgrebene kan indsamle tilstrækkelige beviser.

2013

I 2013 skete der endnu en udvidelse af rpl. § 799, hvor formålet var at "gennemføre en række initiativer, som [skulle] sikre de bedst mulige betingelser for at forebygge, efterforske og retsforfølge økonomisk kriminalitet."[229] Da fokus nu b.la. var på økonomisk kriminalitet blev det muligt at foretage hemmelig ransagning ved tyveri af grov beskaffenhed, jf. strfl. § 286, stk. 1, jf. § 276. Årsagen til denne specifikke udvidelse var en stigning af "anmeldelser om indbrud i privat beboelse på Sjælland samt en øget professionalisme og organisering af indbrudskriminalitet"[230]. Politiets efterforskning i disse sager ville primært rette sig mod at afdække de mistænktes lagre, hvor eventuelle tyvekoster befandt sig. Hemmelig ransagning ved tyveri af grov beskaffenhed, jf. strfl. § 286, stk. 1, jf. § 276, synes derved i første omgang at rette sig mod fysiske husrum.

Udvidelsen blev også begrundet med, at der ikke hidtil havde været hjemmel til hemmelig ransagning ved de kriminalitetstyper der blev tilføjet - dette kunne medføre, at politiet måtte afstå fra almindelig ransagning i den tidlige del af efterforskningsprocessen, for ikke at kompromittere efterforskningen[231]. Resultatet heraf kunne være, at genstande fra kriminelle handlinger ikke kunne sikres som beviser. Rigsadvokaten argumenterede for udvidelsen ud fra en præmis om, at det ikke var afgørende, hvilken kriminalitetstype sagen omhandlede, så længe der ved kriminaliteten opnås et stort udbytte[232]. Han fandt endvidere, at de "karakteristika, der tidligere primært kendetegnede narkotikakriminalitet, nu i højere grad også synes at passe på andre kriminalitetsformer, herunder organiseret indbrudskriminalitet, der ofte er planlagt og målrettet mod særlige værdier, (...), og organiseret af en flerhed af personer, (...)"[233].

[229] LFF 2013-02-28 nr. 164, alm. bem., pkt. 1.1
[230] Ibid. alm. bem., pkt. 5.2.1
[231] LFF 2013-02-28 nr. 164, alm. bem., pkt. 5.2.1
[232] Ibid. alm. bem., pkt. 5.2.1
[233] Ibid. alm. bem., pkt. 5.2.1

5.2.1 Retssikkerhedsmæssige overvejelser

2016

I 2016 blev der ved lovudkast L 105[234], lagt op til en ændring af rpl. § 799, hvorefter det var meningen, at bestemmelsen også skulle komme til at omfatte strfl. § 286, stk. 2. Dette ville have medført, at indgrebet kunne foretages ved en række grove berigelsesforbrydelser, herunder databedrageri af grov beskaffenhed, jf. strfl § 286, stk. 2, jf. § 279 a. Årsagen til, at lovudkastet blev fremsat var, at Rigsadvokaten havde henledt Justitsministeren opmærksomhed på "at mange kriminelle handlinger i stadig større udstrækning foretages digitalt, og at efterforskningen af disse handlinger derfor også foregår digitalt."[235] Rigsadvokaten anførte i den forbindelse, at dette kunne medføre efterforskningsmæssige udfordringer, eftersom retsplejelovens regler om tvangsindgreb muligvis ikke har fulgt med den teknologiske udvikling[236]. Sigtet med lovudkastet var at give adgang til hemmelig ransagning ved økonomisk kriminalitet, også når denne kriminalitet begås på internettet. Imidlertid udgik forslaget til ændringen af rpl. § 799 fra det samlede lovforslag[237], der også indeholdt forslag til andre ændringer af bestemmelser i retsplejeloven og andre love.

5.4.1 Høringssvar til L 105[238]

I forbindelse med lovudkast L 105[239], blev der fremsat kritik i nogle af høringssvarene. Ifølge Justitsministeren ville indførelsen af strfl. § 286, stk. 2 i rpl. § 799 være, "en naturlig tilpasning af bestemmelsen [om hemmelig ransagning], der allerede (...) omfatter narkotikasager og grove sager om tyveri."[240] Forslaget om at ændre rpl. § 799 blev imidlertid udtaget af lovforslaget[241], hvilket muligvis skete på baggrund af disse kritiske høringssvar.

Et af de kritiske høringssvar blev fremsat af Institut for Menneskerettigheder. Baggrunden for deres kritik af udvidelsen var, at "hemmelig ransagning [oprindeligt] var begrænset til de mest alvorlige forbrydelser."[242] Ifølge Institut for Menneskerettigheder er bestemmelsen blevet udvidet betydelig, hvilket er en bekymrende udvilkling da den nu også omfatter ikke-

[234] Lovudkast L 105, 14. oktober 2016
[235] Lovudkast L 105, 14. oktober 2016, alm. bem., pkt. 2.7.2
[236] Lovudkast L 105, 14. oktober 2016, alm. bem., pkt. 2.7.2
[237] Høringsoversigt til lovudkast L 105, 8. december 2016, pkt. 3. Lovforslaget, pkt. 4
[238] Lovudkast L 105, 14. oktober 2016
[239] Lovudkast L 105, 14. oktober 2016
[240] Bilag 4
[241] Høringsoversigt til lovudkast L 105, 8. december 2016, pkt. 3. Lovforslaget, pkt. 4
[242] Bilag 4

personfarlig kriminalitet[243]. Instituttets bekymring følger af, at de anser indgrebet for at være meget alvorligt, hvorfor det kan være betænkeligt at anvende det ved efterforskning af ikke-personfarlig kriminalitet, der synes at være mindre alvorlig[244].

Landsforening for Forsvarsadvokater anser ligeledes udvidelsen af muligheden for hemmelig ransagning for en bekymrende udvikling, da det oprindeligt var forbeholdt specifikke alvorlige forbrydelser[245]. De anfører at "hemmelig ransagning er et indgribende efterforskningsskridt, hvor der over for hensynet til effektiv kriminalitetsbekæmpelse er tungtvejende hensyn til individets retssikkerhed."[246] Problematikken angår ifølge foreningen ikke, hvorvidt indgrebet kan anvendes ved ikke-personfarlig kriminalitet eller ej[247]. De vurderer derimod, at det er problematisk, at udvidelsen af bestemmelsen ikke bliver behandlet særskilt, men "nærmest som en sidebemærkning i et lovforslag"[248]. De mener derfor, at "spørgsmålet om udvidelse af adgangen til hemmelig ransagning bør udsættes til et senere særskilt lovforslag"[249], og behandles mere dybdegående.

Lovudkastets behandling i folketinget

Under behandling i Folketinget blev der stillet spørgsmålstegn ved, hvorfor forslaget om udvidelse af rpl. § 799 til at omfatte strfl. § 286, stk. 2, pludselig var udgået fra det samlede lovforslag[250]. Ordfører Lisbeth Bech Poulsen udtalte i den forbindelse, at "det jo er meget spændende, hvad der er blevet af det med hemmelige ransagninger. Der står en enkelt sætning på [bagerste] side om, at det er udgået. Ministeren kunne måske oplyse os om, hvorfor det er udgået."[251] Justitsminister Søren Pape Poulsen svarede, at "når man udvider anvendelsen af indgreb som f.eks. hemmelige ransagninger, så skal man jo overveje det særlig grundigt og også overveje, om det hører til i en sag som den her, hvor man samler rigtig mange områder."[252]

[243] Bilag 4
[244] Bilag 4
[245] Bilag 4
[246] Bilag 4
[247] Bilag 4
[248] Bilag 4
[249] Bilag 4
[250] Høringsoversigt til lovudkast L 105, 8. december 2016, pkt. 3. Lovforslaget, pkt. 4
[251] https://www.ft.dk/samling/20161/lovforslag/L105/BEH1-42/forhandling.htm, kl. 11:38 (tilgået d. 16/5-19)
[252] https://www.ft.dk/samling/20161/lovforslag/L105/BEH1-42/forhandling.htm, kl. 11:53 (tilgået d. 16/5-19)

Ud fra Søren Pape Poulsens kommentar, tyder det på, at han har taget Landsforeningen for Forsvarsadvokaters henstilling til efterretning.

5.3 Nugældende retstilstand ved hemmelig ransagning

Efter nugældende retstilstand er der hjemmel til hemmelig ransagning ved tyveri af grov beskaffenhed, jf. strfl. § 286, stk. 1, jf. § 276, men ikke ved databedrageri af grov beskaffenhed, jf. strfl. § 286, stk. 2, jf. § 279 a. Siden indførelsen af rpl. 799 i 1997, har udvidelserne af bestemmelsen været et resultat af kriminalitetsbilledet på tidspunktet for udvidelserne. Overordnet har ændringerne primært haft det formål at udvide politiets mulighed for efterforskning af organiseret kriminalitet, hvor hemmeligholdelse har været nødvendig for ikke at afsløre den igangværende efterforskning.

Det er tankevækkende at problemstillingen omkring bestemmelsens anvendelse i forhold til IT-kriminalitet først bliver påtalt i 2016 ved lovudkast L105[253]. Når det tages i betragtning, at lovgiver ellers har været på forkant med hensyn til at indføre specifikke bestemmelser om IT-kriminalitet[254] - herunder straffelovens bestemmelse om databedrageri - er det bemærkelsesværdigt, at den efterforskningsmæssige del af IT-kriminalitet ikke har været behandlet særligt dybdegående.

Rigsadvokaten anfører, at "det i praksis er problematisk, at der ikke kan foretages hemmelig ransagning ved overtrædelse af straffelovens § 286, stk. 2 [herunder § 279 a], når det er muligt, hvis efterforskningen vedrører overtrædelse af § 286, stk. 1, jf. § 276 (grove tyverisager). [Rigsadvokaten bemærker] også i den forbindelse, at disse kriminalitetstyper i stadig større grad begås digitalt."[255]

Det taler for, at hemmelig ransagning udvides til at omfatte databedrageri af grov beskaffenhed, jf. strfl. § 286, stk. 2, jf. § 279 a, at Justitsministeren ved indførelsen af strfl. § 286, stk. 1, jf. § 276 i rpl. § 799, lagde vægt på forbrydelsen alvor ud fra strafferammen[256]. Dette harmonerer ikke med, at der ved strfl. § 286, stk. 1, jf. § 276 kun kan straffes med fængsel indtil 6 år, hvorimod der efter strfl. § 286, stk. 2, jf. § 279 a kan straffes med fængsel op til 8 år. Hvis dette ræsonnement lægges til grund, burde hemmelig ransagning også kunne finde anvendelse ved

[253] Lovudkast L 105, 14. oktober 2016
[254] Lund Madsen, U.2016B.343, Bedrageri i den digitale virkelighed, s. 1
[255] Lovudkast L 105,14. oktober 2016, alm. bem., pkt. 2.7.2
[256] LFF 2013-02-28 nr. 164, alm. bem., pkt. 5.2.2

databedrageri af grov beskaffenhed, da det ud fra strafferammen må anses for at være en meget grov forbrydelse.

Det taler ligeledes for at lade bestemmelsen omfatte databedrageri af grov beskaffenhed, at rpl. § 799 nu omfatter tilfælde hvor politiet logger på en kommunikationsplatform på internettet med rette koder. Denne form for indgreb retter sig specifikt mod efterforskning på internettet, og kan derfor være meget relevant ved databedrageri.

Modsætningsvis taler det imod at lade rpl. § 799 omfatte strfl. § 286, stk. 2, idet hemmelig ransagning oprindeligt var tiltænkt nogle af de mest alvorlige personfarlige forbrydelser og forbrydelser mod statens sikkerhed. På denne baggrund skulle indgrebet også kun finde anvendelse i absolutte undtagelsestilfælde. Eftersom hemmelig ransagning efter 2013 blev muligt ved tyveri af grov beskaffenhed, har dette argument dog ikke nær så stor vægt længere. Med udvidelsen af bestemmelsen til også at omfatte ransagning på en kommunikationsplatform, ser det ikke længere ud til, at hemmelig ransagning kun er forbeholdt de mest alvorlige forbrydelser.

Det nuværende kriminalitetsbillede viser, at økonomisk kriminalitet i stigende grad rykkes på internettet. Man kan ikke komme uden om, at den teknologiske udvikling har skabt muligheder i forbindelse med databedrageri, og det er derfor vigtigt at politiets efterforskningsmuligheder kan følge med denne udvikling.Vi tilslutter os dog Søren Pape Poulsens og Landsforening for Forsvarsadvokaters synspunkt om, at udvidelse af muligheden for at foretage hemmelige ransagninger skal behandles særskilt og mere dybdegående. Dette begrundes ud fra et retssikkerhedsmæssigt hensyn, idet hemmelig ransagning må anses for at være et alvorligt indgreb. Enhver udvidelse må derfor overvejes nøje, da hensynet til en effektiv efterforskning modsvares af hensynet til individets grundlovssikrede rettigheder. Dette skal sammenholdes med, at indgrebet ved indførelsen var forbeholdt absolutte undtagelsestilfælde, hvorfor det må vurderes, om det er hensigtsmæssigt, at bestemmelsen udvides.

Udvidelsen af hemmelig ransagning, til at omfatte strfl. § 286, stk. 2, blev fjernet fra det samlede lovforslag, med en antydning om, at det ville blive behandlet i forbindelse med lovgivning omkring rocker-bande kriminalitet[257]. Det er kritisabelt, at der i 2019 endnu ikke er lagt op til en særskilt og dybdegående behandling af spørgsmålet. Spørgsmålet bør i hvert

[257] https://www.ft.dk/samling/20161/lovforslag/L105/BEH1-42/forhandling.htm, kl. 11:53 (tilgået d. 16/5-19)

tilfælde diskuteres med hensyn til, om der skal ske en udvidelse af den nuværende bestemmelse om hemmelig ransagning så den finder anvendelse ved databedrageri af grov beskaffenhed, jf. strfl. § 286, stk. 2, jf. § 279 a.

5.4 Groft tyveri eller skimming af grov beskaffenhed som forudgående stadie til databedrageri

I ovenstående afsnit bliver lovudkast L 105[258] diskuteret i forhold til, om strfl. § 286, stk. 2 bør være omfattet af rpl. § 799. Lovudkastet L 105 behandler ikke muligheden for hemmelig ransagning ved skimming af grov beskaffenhed, jf. strfl. § 301, stk. 2, jf. stk. 1. Det er interessant at undersøge, om formålet med rpl. § 799 tilsiger, at indgrebet også bør kunne anvendes ved denne kriminalitetstype. Dette skyldes, at både ved strfl. §§ 276 og 301 kan databedrageri være endemålet. Det er derfor bemærkelsesværdigt, at der ved tyveri af grov beskaffenhed, kan ske hemmelig ransagning efter rpl. § 799, men at dette ikke er tilfældet ved skimming af grov beskaffenhed.

5.4.1 Organiseret kriminalitet

Formålet med rpl. § 799 om hemmelig ransagning er primært at give politiet mulighed for at efterforske forbrydelser der begås af flere i forening, uden at bagmænd advares, og derved vanskeliggør eller umuliggør den videre efterforskning. Bestemmelsens sigte er dermed at ramme mere organiseret kriminalitet, og gøre det muligt både at anholde de der udfører forbrydelsen og bagmændene der står for planlægningen.

Hvis formålet med rpl. § 799, sammenholdes med retspraksis angående skimming af grov beskaffenhed, jf. strfl. § 301, stk. 2, jf. stk. 1, kan det i dommene ses, at der ved strafudmålingen lægges vægt på, at forbrydelserne er af organiseret karakter. Et eksempel herpå er dommen TfK 2018.751 V, hvor landsretten anførte, at "forholdene var (...) begået i forening, og der var tale om meget professionel og organiseret kriminalitet (...), ligesom der var opnået et betydeligt udbytte." Retten tillægger også det organiserede element betydning i dommene U 2014.1241

[258] Lovudkast L 105, 14. oktober 2016

V[259], TfK 2015.590 V[260] og TfK 2016.464 V[261] ved strafudmålingen. Sammenlignes dette med dommen TfK 2015.653 V[262], hvor der forud for databedrageri blev begået groft tyveri efter strfl. § 286, stk. 1, jf. § 276, kan det fastslås, at der også i dette tilfælde lægges vægt på forbrydelsens organiserede karakter[263].

Sammenholdes strfl. § 286, stk. 1, jf. 276 og strfl. § 301, stk. 2, jf. stk. 1, med hinanden, kan det lægges til grund, at det tillægges betydning, om kriminaliteten er af organiseret karakter. Ved begge bestemmelser kan endemålet være databedrageri, og sagerne kan derfor minde meget om hinanden, da udførelsen af forbrydelserne typisk har en professionel karakter, er nøje planlagt og udbyttet er omfangsrigt. Forskellen i handlingsforløbet er blot, at der ved tyveri sker fysisk borttagelse af en fremmed rørlig ting, hvorimod der ved skimming, sker anskaffelse mv. af kortoplysninger.

Der er lighedstræk mellem strfl. § 286, stk. 1, jf. § 276 og strfl. og § 301, stk. 2, jf. stk. 1, når forbrydelserne begås forud for databedrageri. Imidlertid fremstår forskellene tydeligt, når baggrunden for muligheden for at foretage hemmelig ransagning ved strfl. § 286, stk. 1, jf. § 276 undersøges.

Hemmelig ransagning ved tyveri af grov beskaffenhed var primært rettet mod at bekæmpe indbrudstyveri af grov beskaffenhed[264]. Fokus var derved på en kriminalitetstype, der adskiller sig meget fra skimming eller tyveri forud for databedrageri. Derfor var det med indførelsen af strfl. § 286, stk. 1, jf. § 276 i rpl. § 799, ikke tiltænkt, at hemmelig ransagning skulle anvendes i forbindelse med tyveri af dankort forud for databedrageri.

[259] Landsretten tilsluttede sig byrettens begrundelse om, at "det [også var] tillagt betydning, at denne kriminalitetstype, der er styret af bagmænd, kan undergrave tilliden til en sikker anvendelse af et sædvanligt betalingsmiddel." Landsretten tilføjede endvidere, at der var "tale om kriminalitet, der [var] nøje planlagt og [havde] en professionel karakter."
[260] Ved strafudmålingen "blev [der] lagt vægt på, at [gerningsmændene] havde handlet under særligt skærpende omstændigheder, da der var tale om nøje planlagt kriminalitet og omfattende og professionelle lovovertrædelser styret af bagmænd og rettet mod et for samfundet vigtigt betalingsmiddel."
[261] Ved strafudmålingen blev det tillagt vægt, "at [tiltalte] havde handlet under særligt skærpende omstændigheder, og at der var tale om nøje planlagt kriminalitet, som havde en professionel og omfattende karakter, og som var rettet mod et for samfundet vigtigt betalingsmiddel."
[262] Vi kunne kun finde en dom, hvor der dømmes for groft tyveri forud for databedrageri, derfor er det svært at fastslå retstilstanden entydigt på baggrund af denne dom
[263] "Landsretten lagde (...) vægt på kriminalitetens omfang og dens professionelle karakter".
[264] LFF 2013-02-28 nr. 164, alm. bem., pkt. 5.2.1

Det fremgår endvidere af forarbejderne til rpl. § 799, at formålet med hemmelige ransagninger ved groft tyveri var at gøre det muligt at foretage fysisk ransagning ved lagre, "uden at det herved [blev afsløret], at der [foregik] en efterforskning mod det organiserede miljø."[265] Muligheden for at foretage hemmelig ransagning af fysiske lokaliteter kan dog også være meget relevant ved skimming f.eks. for at finde beviser i form af frontpaneler eller falske betalingskort. Behovet for at kunne foretage hemmelig ransagning ved skimming, kan derfor også være vigtigt i forhold til at konstatere kriminalitetens omfang, uden at igangværende efterforskning afdækkes.

Ud fra ovenstående kan det konkluderes, at det ikke umiddelbart giver mening, at rpl. § 799 ikke finder anvendelse ved skimming af grov beskaffenhed i forbindelse med databedrageri. Grundlaget for dette fremgår af formålet med indførelsen af bestemmelsen om hemmelig ransagning, som netop er at muliggøre efterforskning af organiseret kriminalitet.

Retspraksis omhandlende skimming af grov beskaffenhed efter strfl. § 301, stk. 2, jf. stk. 1, forud for databedrageri viser, at denne type kriminalitet ofte er af organiseret karakter. Skimming af grov beskaffenhed rammer derved kerneområdet for indgreb efter rpl. § 799. Derudover viser retspraksis, at der har været flere sager omhandlende skimming af grov beskaffenhed forud for databedrageri end sager med groft tyveri forud for databedrageri[266]. Skimming som den forudgående forbrydelse til databedrageri ser derfor ud til at udgøre et større problem end tilfælde, hvor tyveri er den forudgående forbrydelse. Det antages, at problemet forøges ved, at det muligvis er nemmere at indsamle oplysninger gennem skimming end tyveri af betalingskort.

Grundlæggende taler retspraksis for, at muligheden for at foretage hemmelig ransagning udvides til også at omfatte skimming af grov beskaffenhed. Hvis bestemmelsen udvides til at omfatte strfl. § 301, stk. 2, jf. stk. 1, kan tilfælde af organiseret kriminalitet inden for denne kriminalitetstype også bekæmpes ved indgrebet. På denne måde opnås der ensartethed mht. muligheden for at gennemføre indgrebet i forbindelse med tyveri af grov beskaffenhed og skimming af grov beskaffenhed forud for databedrageri. Der kan argumenteres for, at det er underordnet hvilken type kriminalitet der begås ved organiseret kriminalitet, idet der er fælles

[265] LFF 2013-02-28 nr. 164, alm. bem., pkt. 5.2.1
[266] Se f.eks. U 2014.1241 V, TfK 2015.590 V, TfK 2016.464 V og TfK 2018.751 V om skimming af grov beskaffenhed, og TfK 2015.653 V om groft tyveri

kendetegn når kriminaliteten har et organiseret præg[267]. Dette taler også for, at der sker en ensretning af muligheden for at foretage hemmelig ransagning efter rpl. § 799, ved alle former for organiseret kriminalitet.

Alternativt kunne rpl. § 799 ændres, så muligheden for at foretage hemmelig ransagning ved tyveri af grov beskaffenhed ikke længere er til stede. Hvis indgrebet indskrænkes til kun at omfatte de forbrydelser den oprindeligt var tiltænkt, medfører dette, at rpl. § 799 vil være i overensstemmelse med sit oprindelige formål med hensyn til kun at finde anvendelse ved de mest alvorlige kriminalitetstyper.

5.5 Burde bestemmelsen om hemmelig ransagning revideres

Ved kendelsen U 2012.2614 H, bestemte domstolene at politiets adgang til en kommunikationsplatform med rette koder, skal bedømmes efter rpl. § 799 om hemmelig ransagning. Denne kendelse må anses for at have en vigtig præjudikatsværdi for politiets mulighed for at foretage efterforskning på kommunikationsplatforme på internettet. Spørgsmålet var ikke særskilt reguleret i retsplejeloven, og det var derved Højesteret der skabte retstilstanden på området.

Denne situation kan virke problematisk, idet det ikke er Højesterets opgave at udforme retningslinjerne for politiets efterforskning på internettet. Denne opgave tilkommer Folketinget som den lovgivende magt[268]. Når Højesteret tager stilling fra sag til sag angående de efterforskningsmæssige forhold, skabes der ikke klare retningslinjer for politiets efterforskning på internettet. Derudover kan det medføre, at retstilstanden vil komme til at virke vilkårlig. Dette skyldes, at politiet ikke altid vil være i stand til at gennemskue, hvilket indgreb der finder anvendelse, og som følge heraf hvilke betingelser der skal være opfyldt for indgrebet, når efterforskningen foregår på internettet[269]. For at undgå tvivlsspørgsmål om politiets muligheder for at foretage efterforskning på internettet, vil det derfor være fornuftigt at lade lovgiver fastlægge klare retningslinjer omkring dette.

Ved at henføre politiets efterforskningsmetoder på internettet under de eksisterende bestemmelser om tvangsindgreb i retsplejeloven, får disse bestemmelser muligvis et udvidet anvendelsesområde, som ikke oprindeligt var tiltænkt. Dette kan udgøre et problem i forhold

[267] LFF 2013-02-28 nr. 164, alm. bem., pkt. 5.2.1
[268] jf. grundlovens. § 3
[269] Ved U 2012.2614 H blev politiets indgreb kategoriseret som dataaflæsning af by- og landsretten, men Højesteret kategoriserede indgrebet som gentagne hemmelige ransagninger

til rpl. § 799, idet bestemmelsen udover fysisk ransagning nu ved kendelsen U 2012.2614 H, også omfatter kommunikationsplatforme, hvor der logges på med rette koder. Hemmelig ransagning var oprindeligt tiltænkt de mest alvorlige straffelovsovertrædelser[270] - indgrebet skulle kun anvendes i absolutte undtagelsestilfælde og var rettet mod fysiske lokaliteter og genstande. Der kan derfor stilles spørgsmålstegn ved om udvidelsen af rpl. § 799 i U 2012.2614 H er hensigtsmæssig.

Lene Wacher Lentz anfører, at bestemmelsen om dataaflæsning måske ville være mere relevant, hvor politiet logger ind på en kommunikationsplatform med rette koder. Hun lægger op til, at der sker en lovregulering af forholdet, da det "forekommer (...) mest hensigtsmæssigt, at retsplejelovens § 791 b ændres, så bestemmelsen også omfatter dataaflæsning med rette kode."[271] Denne lovregulering vil ifølge hende "skabe klarhed og overensstemmelse mellem [hemmelig ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning]."[272] Dette begrunder hun med, at "hemmelig ransagning [derved vil] bibeholde den beskyttelsesinteresse, [som indgrebet] fortrinsvis var tiltænkt - borgerens bolig og aflåste genstande - og indgreb i meddelelseshemmeligheden forbeholdes de situationer, der kræver bistand fra teleselskaber, postvirksomheder og internetudbydere"[273].

Efter den nuværende retstilstand er det muligt at foretage dataaflæsning, jf. rpl. § 791 b, ved databedrageri af grov beskaffenhed. Det er derimod ikke muligt at logge på en kommunikationsplatform med rette kode ved databedrageri af grov beskaffenhed, da dette er omfattet af rpl. § 799. Denne retstilstand synes besynderlig, idet der ved både dataaflæsning og hemmelig ransagning af kommunikationsplatform kan opnås de samme oplysninger. Indgrebene kan minde meget om hinanden, det er blot metoderne til at opnå oplysninger, der er forskellige. Endvidere kan der ved dataaflæsning ske installation af udstyr på mistænktes computer, og i kendelsen om dataaflæsning ligger der derved en implicit adgang for politiet til at bryde ind i husrum og installere dette udstyr[274]. På baggrund af dette forekommer det modstridigt, at der ved databedrageri af grov beskaffenhed ikke kan foretages indgreb ved at logge på kommunikationsplatform med rette kode. Hemmelig ransagning på internettet synes ikke mere indgribende end dataaflæsning, hvorfor adgangen til at foretage indgrebet ikke burde

[270] Dette omfattede strfl. kap. 12 og 13 og §§ 191, 237, jf. LFF 1996-11-28, nr. 98, de specielle bemærkninger til rpl. § 799
[271] Juristen nr. 1 2016, s. 10
[272] Juristen nr. 1 2016, s. 10
[273] Juristen nr. 1 2016, s. 10
[274] LFF 2001-12-13 nr. 35, de specielle bemærkninger til rpl. § 791 b

være mere indskrænket end muligheden for at foretage dataaflæsning. Ved at rpl. § 791 b ændres til at omfatte dataaflæsning med rette kode, kan ovenstående problemstilling undgås.

Afslutningsvis kan det konkluderes, at muligheden for at logge på en kommunikationsplatform med rette kode, kan reguleres på flere måder. Lene Lentz Wacher argumenter for, at indgrebet bliver henført under rpl. § 791 b, om dataaflæsning. Vi tilslutter os hendes synspunkt, da indgrebene minder om hinanden og begge kan være relevante ved den samme type kriminalitet. Vi mener ikke, at det vil være hensigtsmæssigt at udvide rpl. § 799 om hemmelig ransagning, da dette ikke vil være i overensstemmelse med indgrebets oprindelige formål. På baggrund af indgrebets alvor, bør det kun anvendes efter det tiltænkte formål, og rpl. § 799 bør derved revideres så den kun omfatter de mest alvorlige kriminalitetstyper. Dette tilsiger, at der også bør ske en revidering af rpl. § 791 b, så dette indgreb kommer til at omfatte tilfælde, hvor politiet logger på en kommunikationsplatform på internettet med rette koder.

Kapitel 6 – Konklusion

Indførelsen af strfl. § 279 a har medført både materielle og processuelle udfordringer. De materielle udfordringer er afklaret i retspraksis. Modsat forholder det sig med de processuelle udfordringer, der endnu ikke er blevet dybdegående behandlet, hverken i retspraksis eller juridisk litteratur.

Afgrænsningen mellem strfl. §§ 279 a og 279, 276 og 301

Strfl. § 279 a udspringer af strfl. § 279, om bedrageri, derfor er der ligheder mellem bestemmelsernes formulering og gerningsindhold. Ud fra betænkning nr. 1032/1985, skal afgrænsningen mellem bestemmelserne findes ud fra den menneskelige involvering i det kriminelle handlingsforløb. Således kan det fastslås, at strfl. § 279 a finder anvendelse, hvor den menneskelige involvering er minimal, og hvor der i overvejende grad sker "indgreb i grundlaget for (...) elektronisk databehandling."[275]

Ud fra en analyse af retspraksis kan det udledes, at der har været tvivl om anvendelsesområdet for strfl. § 279 a, ved misbrug af betalingskort. Årsagen til denne tvivl anses for at være et udslag af Vagn Greves kommentar til strfl. § 279 a. Som et resultat af dette henførte anklagemyndigheden indtil dommen U 2014.1688 V misbrug af betalingskort under strfl § 276, da der blev lagt vægt på, at der i hændelsesforløbet skete borttagelse af fremmed rørlig ting Efter dommen U 2014.1688 V må afgrænsningen mellem strfl. §§ 276 og 279 a anses for at være klar. Efterfølgende tiltalepraksis viser, at der ved misbrug af betalingskort rejses tiltale efter strfl. § 276 for det indledende tyveri af betalingskort og strfl. § 279 a for den efterfølgende uberettigede anvendelse af betalingskortet.

Forud for databedrageri kan der i stedet for tyveri af betalingskort ske anskaffelse mv. af betalingskortoplysninger, jf. strfl. § 301. Afgrænsningen mellem strfl. §§ 301 og 279 a er blevet diskuteret i den juridiske litteratur i forhold til, om strfl. § 301 absorberes af strfl. § 279 a, jf. § 21. På baggrund af forarbejderne til strfl. § 301 og tiltalepraksis kan det konkluderes, at afgrænsningen mellem strfl. §§ 301 og 279 a, jf. § 21 skal findes i fortsættes konkretisering i henhold til brug af betalingskortoplysninger - dette betyder at der kun straffes efter strfl. § 301,

[275] Betænkning nr. 1032/1985, de specielle bemærkninger til § 279 a

hvis forsættet ikke er konkret, mens der straffes i sammenstød ved strfl. §§ 301 og 279 a, jf. § 21, hvis forsættet er konkret.

Er reglerne om hemmelig ransagning hensigtsmæssige ved databedrageri

Afgrænsningen mellem ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning har betydning, fordi der ikke er hjemmel til hemmelig ransagning ved databedrageri. Det kan fastslås, at afgørende for hvilket indgreb der finder anvendelse er måden, som politiet får adgang til oplysningerne på og om oplysningerne er undervejs i en kommunikationslinje eller ej.

Det oprindelige formål med rpl. § 799 var, at kunne foretage dette indgreb i absolutte undtagelsestilfælde ved specifikke grove straffelovsovertrædelser. Behovet for indgrebet blev begrundet med, at hemmeligholdelse kunne være nødvendigt i forhold til igangværende efterforskning, for ikke at underrette medgerningsmænd ved kriminalitet af organiseret karakter. Årsagen til, at muligheden for hemmelig ransagning blev udvidet til at omfatte strfl. § 286, stk. 1, jf. § 276, skyldes kriminalitetsbilledet på daværende tidspunkt, hvor en bølge af indbrudstyverier fandt sted i Danmark. Ud fra nuværende kriminalitetsbillede, hvor økonomisk kriminalitet i stigende grad rykker på internettet - og det forhold at denne kriminalitetstype ofte har et organiseret element - kan det fastslås, at formålet med rpl. § 799 også vil være opfyldt ved grov skimming eller databedrageri af grov beskaffenhed. På baggrund af en analyse af lovudkast L 105[276], er årsagen til at rpl. § 799 ikke finder anvendelse ved strfl. § 301, stk. 2, jf. stk. 1 og strfl. § 286, stk. 2, jf. § 279 a, en tilbageholdenhed fra lovgivers side med at udvide anvendelsesområdet for hemmelig ransagning, da indgrebet anses for at være et alvorligt.

Vi mener ikke, at rpl. § 799 bør udvides til at omfatte yderligere kriminalitetstyper. Dette synspunkt sammenholder vi med bestemmelsens oprindelige formål. Derudover anser vi fysisk hemmelig ransagning for et meget alvorligt indgreb, pga. den krænkelse der ligger heri og at individet ikke har mulighed for at overvære indgrebet.

Med kendelsen U 2012.2614 H blev anvendelsesområdet for rpl. § 799 udvidet til også at omfatte muligheden for at logge på en kommunikationsplatform på internettet med rette koder. Dette indgreb anser vi ikke for at være nær så voldsomt som fysisk hemmelig ransagning, hvorfor muligheden for at foretage indgrebet ikke bør være så indskrænket som ved fysisk

[276] Lovudkast L 105, 14. oktober 2016

hemmelig ransagning. På baggrund af dette mener vi, at muligheden for at logge på en kommunikationsplatform på internettet bør henføres under rpl. § 791 b, om dataaflæsning. Dette begrundes med, at indgrebet minder meget om dataaflæsning efter rpl. § 791 b og indgrebet derfor anses for at være relevant ved de samme straffelovsovertrædelser som dataaflæsning. Ved at henføre indgrebet under rpl. § 791 b, vil politiets muligheder for efterforskning på internettet i dette tilfælde blive tydeliggjort, ensartet og strømlinet.

Litteraturliste

Juridiske artikler

- Carlsen, Bent og Michael Elmer, *Datakriminalitet*, Juristen 1986
- Langsted, Lars Bo, *Dankortet i strafferetlig belysning,* U.2019B.48
- Lentz, Lene Wacher, *Hemmelig ransagning og brevstandsning i den digitale virkelighed*, Juristen nr. 1, 2016
- Madsen, Lasse Lund, *Bedrageri i den digitale virkelighed*, U.2016B.343

Juridisk litteratur

- Greve, Vagn, *EDB-strafferet*, Jurist- og Økonomforbundets Forlag, 2. reviderede udgave (1986)
- Greve, Vagn, Poul Dahl Jensen, Gorm Toftegaard Nielsen, *Kommenteret straffelov, Speciel del,* Jurist- og Økonomforbundets Forlag, 10. omarbejdede udgave (2012)
- Heine, Kasper, Martin von Haller Grønbæk, Jan Trzaskowski, *Internetjura*, Forlaget Thomson, 2. udgave (2002)
- Kistrup, Michael, Jakob Lund Poulsen, Jens Røn, Thomas Rørdam, *Straffeprocessen*, Karnov Group, 3. udgave (2018)
- Lentz, Lene Wacher, *Efterforskningens grænser på internettet* (s. 137-151). I Rikke Frank Jørgensen og Birgitte Kofod Olsen (red.), *Eksponeret - Grænserne for privatliv i en digital tid*, Gads Forlag, 1. udgave, (2018)
- Munk-Hansen, Carsten, *Retsvidenskabsteori*, Jurist- og Økonomforbundets Forlag, 1. udgave (2014)
- Møller, Jens, Oliver Talevski, Peter Thønnings og Ulrik Rammeskow Bang-Pedersen (red.), *Kommenteret retsplejelov, Bruxelles I-forordningen*, *Bind III §§ 683-1043,* Jurist- og Økonomforbundets Forlag, 10. udgave (2018)
- Nielsen, Gorm Toftegaard, Thomas Elholm, Morten Niels Jakobsen, *Kommenteret straffelov, Speciel del*, Jurist- og Økonomforbundets Forlag, 11. omarbejdede udgave (2017)
- Røn, Jens, *Databedrageri - stadig en overset bestemmelse?* (s. 295-308), I Sten Bønsing, Thomas Elholm, Søren Sandfeld Jakobsen og Lene Wacher Lentz (red.), *I forskningens og formidlingens tjeneste - festskrift til professor Lars Bo Langsted,* Ex Tuto Publishing, 1. udgave (2018)

- Waaben, Knud v/ Lars Bo Langsted, *Strafferettens almindelige del I, Ansvarslæren,* Karnov Group, 5. reviderede udgave (2011)
- Waaben, Knud v/ Lars Bo Langsted, *Strafferettens specielle del*, Karnov Group, 6. reviderede udgave (2014)

Forarbejder

- Betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter
- Betænkning nr. 1032/1985 om datakriminalitet
- Betænkning nr. 1159/1989 om ransagning under efterforskning
- Betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning
- Betænkning nr. 1417/2002 om IT-kriminalitet
- LFF 1985-04-24 nr. 221, Forslag til Lov om ændring af straffeloven (Datakriminalitet)
- LFF 1996-11-28 nr. 98, Forslag til Lov om ændring af straffeloven, retsplejeloven og våbenloven (Styrkelse af politiets muligheder for at efterforske alvorlig kriminalitet, konfiskation, øget vidnebeskyttelse og skærpelse af straffen for våbenbesiddelse m.v.)
- LFF 2001-12-13 nr. 35, Forslag til lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.)
- LFF 2003-11-05 nr. 55, Forslag til lov om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.)
- LFF 2013-02-28 nr. 164, Forslag til lov om ændring straffeloven, retsplejeloven og forskellige andre love (Styrket indsats over for økonomisk kriminalitet)

Lovgivning

- Den Europæiske Menneskerettighedskonvention, jf. lovbekendtgørelse L 1998-10-19 nr. 750 med senere ændringer
- Grundloven, jf. lov 1953-06-05, nr. 169
- Retsplejeloven, jf. lovbekendtgørelse L 2018-11-14, nr. 1284 med senere ændringer
- Straffeloven, jf. lovbekendtgørelse L 2018-09-20, nr. 1156 med senere ændringer

Retspraksis

Anklagemyndighedens vidensbase

- AM2013.03.18B

Tidsskrift for Kriminalret

- TfK 2009.48 Ø
- TfK 2011.388 Ø
- TfK 2015.289 Ø
- TfK 2015.443 Ø
- TfK 2015.590 V
- TfK 2015.653 V
- TfK 2016.464 V
- TfK 2018.751 V

Ugeskrift for Retsvæsen

- U 1998.1613 Ø
- U 1999.178 V
- U 1999.985 H
- U 2001.1980/2H
- U 2008.1734 V
- U 2012.2614 H
- U 2014.1241 V
- U 2014.1688 V

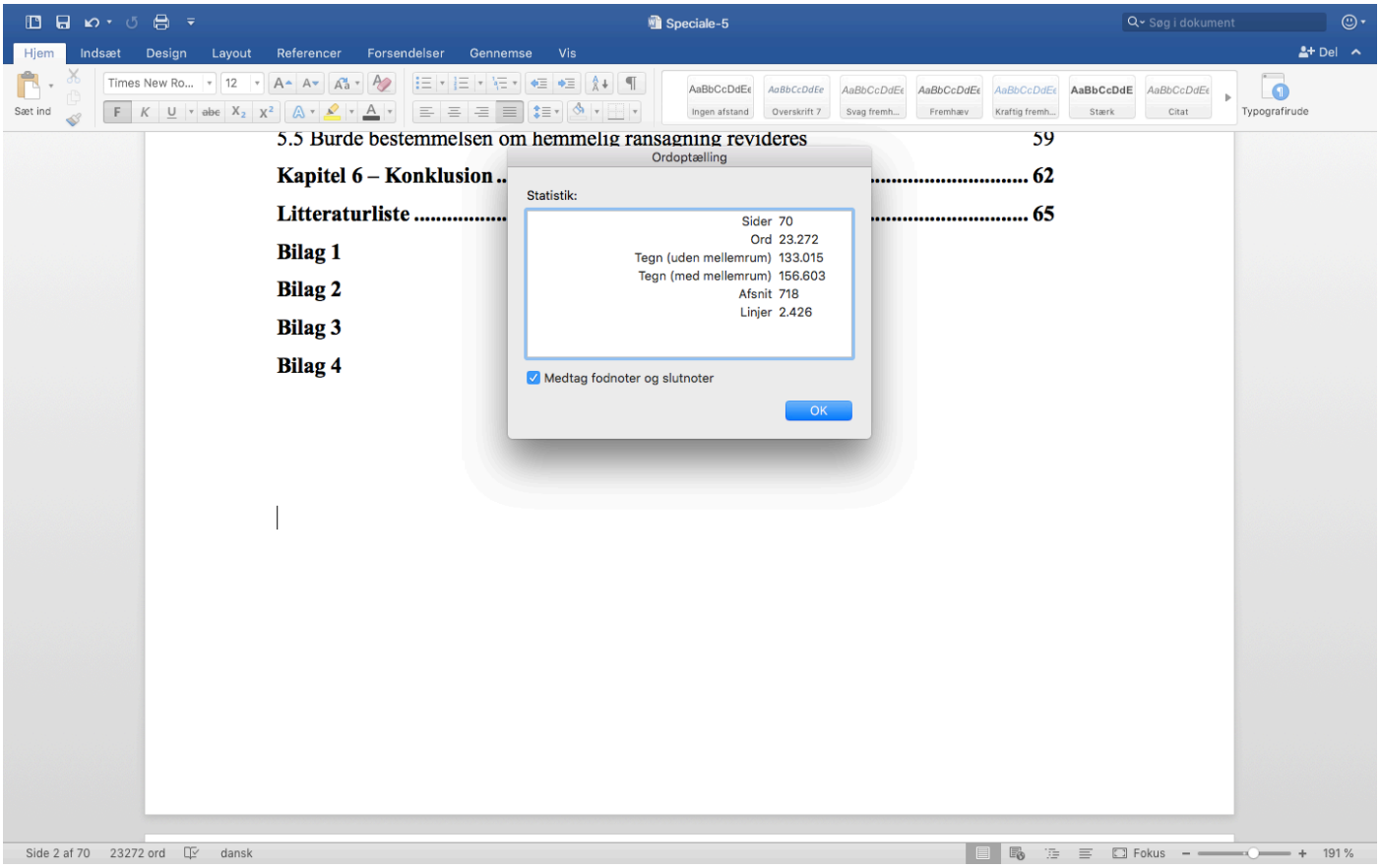
Links

- Anker, Nina Donovan og Sofie Ramsrud Jensen, Moderne berigelseskriminalitet - En dybdegående analyse af straffelovens § 279 a, Speciale Københavns Universitet (2018):http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Prisopgaver/bedste_opg_2018.pdf, (tilgået d. 16/5-2019)
- http://nyheder.tv2.dk/tech/2016-08-12-pcen-fylder-35-aar-var-taet-paa-ikke-at-lykkes, (tilgået d. 16/5-2019)
- https://politi.dk/rigspolitiet/nyhedsliste/nyt-center-skal-bekaempe-it-relateret-oekonomisk-kriminalitet/2019/01/08, (tilgået d. 16/5-2019)
- https://www.berlingske.dk/samfund/politiet-faar-friere-haender-til-hemmelig-ransagning, (tilgået d. 16/5-2019)

- https://www.ft.dk/samling/20161/lovforslag/L105/BEH1-42/forhandling.htm, (tilgået d. 16/5-2019)
- http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Prisopgaver/bedste_opg_2018.pdf, (tilgået d. 16/5-2019)
- https://www.oxfordlearnersdictionaries.com/definition/english/protocol?q=protocol, (tilgået d. 16/5-2019)

Andet

- Det Kriminalpræventive Råd, *Når forbrydelser bliver digitale, en antologi om IT-kriminalitet og adfærd på internettet*, marts 2016
- Høringsoversigt til lovudkast L 105, Kommenteret oversigt over høringssvar vedrørende forslag til Lov om ændring af retsplejeloven, lov om fuldbyrdelse af straf m.v. og lov om elektroniske kommunikationsnet og -tjenester (Udeblivelsesdomme, forkyndelse og anvendelse af digital kommunikation i straffesager m.v.), 8. december 2016
- Kruize, Peter, Det Kriminalpræventive Råd, Internetkriminalitet 2017. Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace, Det Juridiske Fakultet, Københavns Universitet, maj 2018
- Lovudkast nr. L 105, Forslag til Lov om ændring af retsplejeloven, lov om fuldbyrdelse af straf m.v. og lov om elektroniske kommunikationsnet og -tjenester (Udeblivelsesdomme, forkyndelse og anvendelse af digital kommunikation i straffesager m.v.), 14. oktober 2016


Speciale-5
Søg i dokument
Hjem
Indsæt
Design
Layout
Referencer
Forsendelser
Gennemse
Vis
Del
Sæt ind
Times New Ro...
12
Ingen afstand
Overskrift 7
Svag fremh...
Fremhæv
Kraftig fremh...
Stærk
Citat
Typografirude
5.5 Burde bestemmelsen om hemmelig ransagning revideres 59
Kapitel 6 – Konklusion ... 62
Litteraturliste ... 65
Bilag 1
Bilag 2
Bilag 3
Bilag 4
Ordoptælling
Statistik:
Sider 70
Ord 23.272
Tegn (uden mellemrum) 133.015
Tegn (med mellemrum) 156.603
Afsnit 718
Linjer 2.426
Medtag fodnoter og slutnoter
OK
Side 2 af 70
23272 ord
dansk
Fokus
191 %