Grensene mellom databedrageri, alminnelig bedrageri og tyveri

En analyse av straffeloven § 371 bokstav b opp imot § 371 bokstav a og § 321

Kandidatnummer: 104

Antall ord:14 943

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. mai 2023

Innholdsfortegnelse

Forord

Masteroppgaveprosessen har vært krevende – varme takk til mamma og pappa for uvurderlig støtte fra sidelinjen. Mange takk også til roomie for mer enn nok rom til å tenke høyt.

1 Problemstilling

Hensikten med masteroppgaven er en analytisk sammenligning og oversikt de lege lata av handlinger som subsumeres under straffelovens bestemmelser om databedrageri, alminnelig bedrageri og tyveri. Kripos-rapporten *Cyberkriminalitet 2023* peker på at den teknologiske utviklingen har ført til at datakriminalitet er en økende trussel i dagens samfunn.[1] Databedrageribestemmelsen i straffeloven § 371 bokstav b er et av verktøyene i kampen mot slik kriminalitet.[2] For at databedrageribestemmelsen skal være et effektivt verktøy er det imidlertid nødvendig at rettsanvenderen bruker bestemmelsen på de tilfellene den er ment å ramme.

Spørsmålet er hva som karakteriserer handlingene som faller inn under databedrageribestemmelsen, jf. strl. § 371 bokstav b, og hvordan de skiller seg fra handlingene som faller inn under enten den alminnelige bedrageri- eller tyveribestemmelsen, jf. henholdsvis strl. § 371 bokstav a og § 321.

Rettspraksis viser nemlig at forholdet mellom databedrageri- og tyveribestemmelsen kan være utfordrende for påtalemyndigheten, forsvarere og domstolene. Slik presentasjonen og redegjørelsen av bestemmelsene i kapittel 2 viser, tilsier bestemmelsenes ordlyd at visse handlinger tilsynelatende skal behandles etter databedrageribestemmelsen. Øvrige rettskilder trekker derimot i retning av anvendelse av tyveribestemmelsen. Attpåtil avslører rettspraksis og juridisk teori, at valget mellom databedrageri og alminnelig bedrageri kan være vanskelig. Masteroppgaven er derfor tiltenkt som et hjelpemiddel i målet om rett subsumsjon.

[1] Kripos – den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet, *Cyberkriminalitet 2023: Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer* (Kripos ved Politidirektoratet, 2023), side 6. Se <https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf> for PDF-versjon av rapporten, besøkt 7. mai 2023

[2] Lov 20. mai 2005 nr. 28 om straff (straffeloven – strl.); Norge er ved European Cyber Crime Convention (ETS No. 185 2001) internasjonalt forpliktet til å ha prosessuelle og materielle bestemmelser om datakriminalitet, og konvensjonens artikkel 8 pålegger en plikt om å ha en bestemmelse om databedrageri, se Andrej Saving, *EU Internet Law: Second Edition* (Cheltenham, UK, Edward Elga Publishing 2017) s. 331-331; Inger Marie Sunde, «Har vi behov for straffebud om datakriminalitet?» (2019) i Tidsskrift for strafferett 19(2), 168-185, s. 169. Den norske databedrageribestemmelsen kom imidlertid ikke til som følge av konvensjonen, ettersom den norske databedrageribestemmelsen ble vedtatt i 1987 og dermed forut for at konvensjonen ble påbegynt og vedtatt, jf. Ot.prp. nr. 40 (2004-2005) punkt 2.1 og ETS No. 185 2001, Explanatory Report.

2 Sammenligning av bestemmelsene

2.1 Tre likheter

Straffeloven § 371 bokstav b, § 371 bokstav a og § 321 er ikke samlet i samme kapittel i straffeloven, likevel er det tre overordnede likheter mellom bestemmelsene. For det første må alle tolkes og anvendes i henhold til det strafferettslige legalitetsprinsippet, deretter har bestemmelsene lik strafferamme, og siste likhet er de to forsettvilkårene – at overtredelse av gjerningsbeskrivelsene må være gjort forsettlig og med forsett om uberettiget vinning.

2.1.1 Legalitetsprinsippet

Det følger av Grunnloven § 96, Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 7 og straffeloven § 14 at bestemmelsene må tolkes og anvendes i henhold til det strafferettslige legalitetsprinsippet.[3]

Det fremgår av Grunnloven § 96 første ledd at «[i]ngen kan dømmes uten etter lov». Tilsvarende fremgår av ordlyden i strl. § 14 som tilsier at adgangen til å ilegge straff forutsetter hjemmel i lov. Hjemmelskranken innebærer ikke bare et lovkrav, men oppstiller også krav til straffebudets utforming og tilgjengelighet, jf. HR-2020-2019-A avsnitt 14. Loven skal derfor være klar, slik at en lett skal kunne gjøre seg kjent med hva som kvalifiserer til overtredelse og at konsekvensene for overtredelse av straffebudet skal være tilstrekkelig forutberegnelig, jf. HR-2020-955-A avsnitt 22.

Norge er folkerettslig forpliktet til EMK, og legalitetsprinsippet må forstås i lys av kravene oppstilt ved EMK artikkel 7. Der fremgår det at straffeadgang forutsetter hjemmel i lov. EMK artikkel 7 skal videre forstås i lys av tilhørende rettspraksis fra Den europeiske menneskerettighetsdomstolen (EMD). I nevnte HR-2020-2019-A gir Høyesterett i avsnitt 15 uttrykk for at klarhetskravet ved Grl. § 96 er sammenfallende med legalitetsprinsippet etter EMK art. 7 og slik det er forstått i EMD-rettspraksis. EMD har fastslått at det å måtte tolke et straffebud etter alminnelig juridisk metode ikke automatisk medfører brudd på art. 7, se for eksempel *Kafkaris v. Kypros* avsnitt 140-141 og *Vasiliaukas v. Litauen* avsnitt 154-155. Det avgjørende for hvorvidt lovtolkningen er i tråd med det strafferettslige legalitetsprinsippet er

[3] Lov 17. mai 1814 Kongeriket Norges Grunnlov

om tolkningsresultatet har «tilstrekkelig forankring» i straffebudet slik at forutberegnelighetskravet er oppfylt og at «bestemmelsens kjerne» består, jf. HR-2020-2019-A avsnitt 17-20.

2.1.2 Lik strafferamme

«med bot eller fengsel inntil 2 år»

Slik lyder angivelsen av strafferammen for overtredelse av de tre bestemmelsene, jf. strl. §§ 371 bokstav b, 371 bokstav a og 321. Bestemmelsene har lik strafferamme, og isolert kan det tilsi at hvorvidt påtalemyndigheten eller domstolene anvender feil bestemmelse, ikke er av betydning.

Derimot, det er ikke bare straffereaksjonen pålagt av staten som kan oppleves som straff for den domfelte. Omgivelsenes reaksjoner og oppfatninger, kan også oppleves om straff. For noen kan det være mer stigmatiserende å bli dømt for bedrageri enn tyveri. Bedrageriets særegne element av «lureri» gjør at det ikke er urimelig å anta at et stempel om å være svikaktig følger vedkommende også etter at hen har sonet straffen sin. Anvendelse av rett straffebud er dermed viktig for den sosiale straffen.

Videre har straffenivå ved domfellelse tradisjonelt vært fastlagt gjennom rettspraksis. Ved straffeloven 2005 ble det imidlertid bestemt at lovgiver gjennom forarbeidene skulle gi føringer for straffenivået.[4] Det fremgår av Ot.prp. nr. 22 (2008-2009) s. 465 at strafferammen for bedrageribestemmelsene ble nedjustert samtidig som databedrageribestemmelsen fikk tilføyd det tredje gjerningsalternativet. Lovendringen ble gjort blant annet for at strafferammen skulle være lik den ved tyveribestemmelsen. Felles for bestemmelsene er at nevnte forarbeid videre uttrykker at straffenivået fastlagt i rettspraksis etter 1902-straffeloven ikke er ment å endres, jf. forarbeidet ss. 451 og 465. Straffenivået beror derfor på tilhørende rettspraksis for hver av bestemmelsene, noe som kan resultere i forskjeller på tross av lik strafferamme i lovteksten. Anvendelse av rett straffebud er dermed viktig for straff etter rett straffenivå.

[4] Magnus Matningsdal, *Norsk spesielle strafferett* (2021, Fagbokforlaget) s. 13

2.1.3 Forsettvilkårene

Domfellelse etter databedrageri, alminnelig bedrageri og tyveri krever alle at overtredelsen av gjerningsbeskrivelsen må være gjort forsettlig jf. strl. § 21 jf. § 371 bokstav a og b og § 321. Videre fremgår det av strl. § 22 at forsettkravet innebærer at gjerningspersonens forsett må dekke alle gjerningselementene i den aktuelle bestemmelsen jf. første ledd, og en eventuell rettsuvitenhet hos gjerningspersonen er ikke til hinder for at handlingen er gjort forsettlig jf. annet ledd. Norsk strafferett opererer med tre alternative forsett, slik at en forsettlig overtredelse må enten være gjort med hensiktsforsett, sannsynlighetsforsett eller dolus eventualis, jf. henholdsvis § 22 første ledd bokstav a, b og c.

I tillegg til at alle gjerningselementene må være overtrådt forsettlig er det ved bestemmelsene krav om at overtredelsen er gjort med «forsett om å skaffe seg eller andre en uberettiget vinning», jf. strl. §§ 371 bokstav a og b og 321. Dette blir tradisjonelt omtalt som krav om «vinningsforsett», og en foretar en forsettvurdering etter kravene til forsett i strl. § 22.

Ordlyden «seg eller andre» innebærer at vinningsforsett foreligger både i de tilfeller der den uberettigede vinningen er for gjerningspersonen selv og der den oppnås for en annen. Videre tilsier ordlyden «uberettiget vinning» en økonomisk fordel som vedkommende ikke har krav på. For eksempel dersom gjerningspersonen har et forfalt pengekrav mot fornærmede, vil det ikke være «forsett om uberettiget vinning» om hen tilegner seg pengene.[5]

Høyesterett har avgjort at kravet om vinningsforsett ikke innebærer at den borttatte eller oppnådde tingen har en selvstendig økonomisk verdi, se Rt. 1975 s. 472. I dommen hadde den tiltalte tatt sjekkblanketter som ikke var ferdig utfylt med hensikt om å senere forsøke å heve penger på sjekkene. Høyesterett ga uttrykk for at kravet om vinningsforsett kan være oppfylt selv hvis den uberettigede vinningen først kan realiseres på et senere tidspunkt, og konkluderte at vinningsforsett ikke innebærer krav om at den uberettigede vinningen må samsvare med et formuestap. En mer dagsaktuell eksemplifisering av Høyesteretts konklusjon er presentert av Matningsdal: Et bankkort har i seg selv neppe en økonomisk verdi, forsett om uberettiget vinning er heller knyttet til den potensielle bruken av kortet.[6]

[5] Magnus Matningsdal, *Norsk spesiell strafferett* (Bergen, 3.utgave, Fagbokforlaget 2021) s. 323
[6] Ibid.

2.2 Databedrageri

Straffeloven § 371 bokstav b:

> *«Med bot eller fengsel inntil 2 år straffes den som med forsett om å skaffe seg eller andre en uberettiget vinning […] bruker uriktig eller ufullstendig opplysning, endrer data eller datasystem, disponerer over et kredittkort eller debetkort som tilhører en annen, eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen.»*

2.2.1 «uberettiget påvirker resultatet av en automatisert databehandling»

Ved fremstillinger av databedrageribestemmelsen i juridisk teori kommer vilkåret «uberettiget påvirker resultatet av en automatisert databehandling» ofte avslutningsvis ved gjennomgangen av gjerningsalternativene, og gjerne sammen med sekkealternativet «på annen måte». En kontekstuell ordlydsforståelse av vilkåret i § 371 bokstav b tilsier imidlertid at det er et fellesvilkår for alle gjerningsalternativene. Overtredelsen av et gjerningsalternativ må medføre at gjerningspersonen «uberettiget påvirker resultatet av en automatisert databehandling». Ot.prp. nr. 22 (2008-2009) s. 327 drøfter tilføyelsen av gjerningsalternativet «disponerer over et kredittkort eller debetkort som tilhører en annen», og at straffansvar ved en slik disposisjon forutsetter at den «derved rettsstridig påvirker resultatet av en automatisert databehandling». Det fremgår av ordlyden sammenholdt med forarbeidsuttalelsen at vilkåret er et fellesvilkår for alle gjerningsalternativene. For videre tolkning av straffebudet er det dermed hensiktsmessig å først klargjøre innholdet i fellesvilkåret.

Ordlyden består av tre hovedelementer; «uberettiget», «påvirker resultatet» og «automatisert databehandling». En alminnelig språklig forståelse av «uberettiget» tilsier at en har handlet uten rett. Ordlyden er imidlertid uklar om hvorvidt dette er avgrenset til lovstridige handlinger. Det fremgår av Ot.prp. nr. 22 (2008-2009) på side 22 at «uberettiget» oppstiller en rettsstridsreservasjon, og skal avgrense hvilke handlinger som er straffbare. Videre viser Justis- og politidepartementet til at de i tidligere forarbeid har fastlagt at rettsstridsreservasjonen skal anvendes der det ikke vil være tilstrekkelig å vise til at en

handling er «ulovlig».[7] Ordlyden «ulovlig» innebærer en avgrensning til rettsforhold regulert av lov eller forskrift. «[U]berettiget» ved § 371 bokstav b er derfor ment å inkludere brudd på privatrettslige avtaler eller instrukser, og ved handlinger som faller utenfor «akseptabel atferd på et bestemt livsområde».[8]

Ordlyden «påvirker resultatet» tilsier et krav om at den uberettigede handlingen har betydning for utfallet av den «automatiserte databehanding[en]». Uttalelser i NOU 1985: 31 på side 33 kan forstås som at gjerningsbeskrivelsen i databedrageribestemmelsen er fullbyrdet idet uriktige data er blitt lagt inn i maskinen eller datasystemet. Høyesterett har imidlertid tilbakevist en slik forståelse i Rt. 1991 s. 532. Ansatte i en datasentral hadde endret data for trygdeutbetaling og slik forsøkt å sørge for at utbetalingene skulle gå til deres personlige kontoer. Datasystemet var imidlertid ikke egnet til å takle beløpets størrelse, og utbetalingene gikk ikke gjennom. Den uberettigede handlingen ble avslørt ved manglende trygdeutbetaling. Høyesterett leste forarbeidet i lys av bestemmelsens ordlyd og uttalte at det «neppe kan ha vært meningen at allerede innmatingen av data uten videre skulle innebære fullbyrdet forbrytelse». I tillegg så førstvoterende straffebudet i sammenheng med at det i den alminnelige bedrageribestemmelsen er krav om at gjerningspersonens handling resulterer i en «forledelse». Konklusjonen ble at det ved databedrageribestemmelsen er krav om at den uberettigede handlingen må ha «frembragt et resultat» for at gjerningsbeskrivelsen skal være overtrådt.[9]

Høyesteretts konklusjon utgjør videre den nedre grensen mot forsøk på databedrageri jf. strl. § 16 jf. strl. § 371 bokstav b. Ettersom de tiltalte i Rt. 1991 s. 532 ikke hadde «frembragt et resultat» var de kun skyldig i forsøk på databedrageri.

Ordlyden «databehandling» vil ved en vid forståelse, tilsi enhver prosessering av informasjon. I snever forstand tilsier ordlyden at et sett av data behandles ved en serie operasjoner i et datasystem.[10] Databehandlingens funksjon beror på dens anvendelsesområde, det er imidlertid ingen holdepunkter ved databedrageribestemmelsens øvrige ordlyd om at det kan oppstilles et spesifikt funksjonskrav ved databehandlingen som påvirkes. Eneste krav er at påvirkningen er «uberettiget». Dermed vil for eksempel både det å sende inn feil opplysninger i et elektronisk

[7] Ot.prp. nr.8 (2007-2008) Om lov om endringer i straffeloven 20. mai 2005 nr. 28 mv.
[8] Ot.prp. nr.22 (2008-2009) s. 22
[9] Rt. 1991 s. 532, på side 534
[10] Eirik Rossen, «databehandling» (*Store norske leksikon*, 22. september 2021) <https://snl.no/databehandling> besøkt 20. februar 2023

trygdeskjema og det å manipulere et datasystem slik at det feilrapporterer grunnlaget for et betalingskrav kunne falle inn under databedrageribestemmelsen.

En alminnelig språklig forståelse av «automatisert» er at noe går av seg selv. I en hverdagslig kontekst omfatter ordlyden både en persons handlingsmønster basert på vane og at et datasystem er forhåndsprogrammert til å behandle informasjon som blir lagt inn eller som allerede er lagret i datasystemet. Et eksempel på sistnevnte er trafikklys med forhåndsprogrammerte intervaller for å regulere et lyskryss.

Konteksten «databehandling» i § 371 bokstav b snevrer inn ordlydsforståelsen, og tilsier at bestemmelsens ordlyd sikter til informasjonsbehandling av forhåndsprogrammert datasystem. Videre tilsier dette at behandlingen av innlagt eller lagret informasjon foregår uten menneskelig medvirkning, det er altså ikke en person som behandler dataen. En slik forståelse sammenfaller med Ot.prp. nr. 35 (1986-1987) side 27 om at avgjørende ved databedrageribestemmelsen er at det ikke er et menneske som forledes, men en datamaskin som «føres bak lyset».[11] Kjernen i databedrageribestemmelsen er derfor manipulering av en datamaskin. Gjerningspersonens uberettigede handling må være rettet mot en ubetjent datamaskin, og et hendelsesforløp som innebærer at en eller flere personer blir forledet faller dermed utenfor gjerningsbeskrivelsen.

2.2.2 … og «derved volder tap eller fare for tap for noen»

Siste fellesvilkår for de alternative gjerningsbeskrivelsene er at den uberettigede påvirkningen av en automatisert databehandling «derved volder tap eller fare for tap for noen».

Ordlyden «derved» tilsier krav om årsakssammenheng mellom gjerningsbeskrivelsen og det frembragte resultatet. Det vil si, handlingen som medfører at en uberettiget påvirker resultatet av en automatisert databehandling må være årsaken til «tap eller fare for tap».

Videre innebærer «tap» lest i kontekst av vilkåret om «uberettiget vinning» at det er tale om økonomisk tap. Det er imidlertid ikke et krav om at økonomisk tap må foreligge, det er tilstrekkelig at en fare for slikt tap har oppstått jf. ordlyden «fare for tap». I Rt. 1994 s. 740 hadde den domfelte begått databedrageri ved å opprette fiktive kontoer i banken hun jobbet i

[11] Se NOU 2002: 4 Ny straffelov, på side 381 fremgår det at det ble foreslått en videreføring av databedrageribestemmelsen i straffeloven 1902 og tidligere forarbeidsuttalelser om straffebud er derfor fremdeles gjeldende.

og innvilget lån til kontoinnehaver. Høyesterett uttalte at det avgjørende for fullbyrdet lovbrudd er at «fare for tap er oppstått» – og det utgjør derfor minimumskravet for fullbyrdet lovbrudd. I 1994-saken viste Høyesterett også til nevnte Rt. 1991 s. 532, og påpekte at de tiltaltes handlinger i 1991-saken ikke hadde «frembragt et resultat» på grunn av at det benyttede datasystemet var uegnet. I den saken medførte derfor ikke innmatingen av data en reell fare for tap. Det vil si, det var det konkrete saksforholdet i 1991-saken som gjorde at innmatingen av data ikke oppfylte kravene for overtredelse av databedrageribestemmelsen. Motsetningsvis, i saken for Høyesterett i 1994 ble tiltalte ikke hindret av et uegnet datasystem, og innmatingen av data frembragte dermed et resultat og gjorde at det oppsto en reell fare for tap. Det er dermed sammenheng mellom kravet om at handlingen må ha «frembragt et resultat» og kravet om at en reell fare er oppstått.

Avslutningsvis er det krav om at tapet eller faren for tap har oppstått «for noen». Ordlyden tilsier at det avgjørende for straffebudets anvendelse er at potensialet for tap faktisk er oppstått, og at det ikke er av betydning *for hvem* potensialet har oppstått. Det samsvarer med forarbeidsuttalelsen på side 26 i Ot.prp. nr. 35 (1986-1987).

2.2.3 De alternative gjerningsbeskrivelsene i § 371 bokstav b

Første gjerningsalternativ i databedrageribestemmelsen er at en «bruker uriktig eller ufullstendig opplysning» til å uberettiget påvirke resultatet av en automatisert databehandling. Alternativet er i Ot.prp. nr. 35 (1986-1987) på side 26 eksemplifisert med at en bruker et bankkort som tilhører en annen til å manipulere en kortautomat til å overføre penger til ens egen konto. Eksempelet ble imidlertid gitt før tilføyelsen av gjerningsalternativet om misbruk av en annens kreditt- og debetkort,[12] og ville med dagens lovgivning trolig vært mer passende som eksempel ved det tilføyde gjerningsalternativet. Tilsvarende oppfatning fremgår av Ot.prp. nr. 22 (2008-2009) side 465 som behandler tilføyelsen til databedrageribestemmelsen. Et annet eksempel som passer ordlyden er en urettmessig utbetaling som følge av at en legger inn feil eller ufullstendige opplysninger i et elektronisk skjema som behandles ved automatisert databehandling. Det kan for eksempel være en leges refusjonssøknad til HELFO eller en arbeidssøkers meldekort til NAV. Fra rettspraksis kan vilkåret eksemplifiseres med Rt. 1990 s. 955. Ved å bokføre fiktive bilag i det databaserte regnskapssystemet hos arbeidsgiveren sørget den domfelte for urettmessige utbetalinger på til sammen 1,2 millioner

[12] Tilføyelsen ble gjort som følge av lovendring, se Ot.prp. nr. 22 (2008-2009) side 465

kroner til egen konto. Fra nyere tid kan vilkåret illustreres ved avgjørelsen om straffeutmåling i HR-2021-2556-A. Innehaveren av en virksomhet hadde sendt inn urettmessige refusjonskrav til NAV for lønn eller andre ytelser etter reglene i midlertidig forskrift om lønnskompensasjon til permitterte for å avhjelpe konsekvenser av covid-19. Refusjonssøknadene ble behandlet ved automatisert databehandling, og vedkommende hadde fremsatt «uriktige opplysninger om arbeidsforhold» ved virksomheten.

Det andre gjerningsalternativet er at en «endrer data eller datasystem». Ordlyden tilsier at en forandrer enten på et informasjonsett eller det installerte systemet på en datamaskin. «[D]atasystem» erstattet den tidligere ordlyden «programutrustning», men utgjorde ikke en realitetsendring jf. Ot.prp. nr. 22 (2008-2009) s. 465. Om «programutrustning» fremgår det av Ot.prp. nr. 35 (1986-1987) s. 26-27 at både fast innlagt og midlertidig «programutrustning» er omfattet av bestemmelsen. Tilsvarende gjelder dermed «datasystem». I juridisk teori eksemplifiserer Matningsdal gjerningsalternativet med nevnte Rt. 1991 s. 532, der de ansatte i en datasentral ved å «endre [på] data» hadde forsøkt å omdirigere trygdeutbetalinger til egen konto.[13]

Et annet eksempel er saksforholdet i Rt. 1995 s. 1872. Ved ulike fremgangsmåter hadde den domfelte oppnådd gratis telefonforbindelse mellom egen datamaskin og datamaskiner eller databaser i både Norge og utland. Felles for fremgangsmåtene redegjort av Høyesterett er at gjerningspersonen skaffet adgang til både andres dataanlegg og til å påvirke andres dataprogram. Blant annet benyttet han andre kunders PIN-koder til oppringing, noe som innebar at han ble påkoblet deres telefonlinjer slik at deres kundeforhold ble belastet med tellerskrittene. Han koblet seg også via grønt nummer til hussentralen til et tjenesteselskap,[14] som gjorde at tellerskrittene ved hans oppringing ble belastet hussentralens abonnement. Tredje fremgangsmåte var viderekobling fra både Televerkets og et biblioteks databaser til egen telefon, og hans oppringinger ble derfor belastet deres telefonregning. De ulike metodene innebar å «endre data eller programutrustning» jf. strl. 1902 § 270 første ledd nr.

[13] Magnus Matningsdal *Straffeloven: De straffbare handlingene: Kommentarutgave* (Oslo, Universitetsforlaget 2017) s. 986

[14] Et «grønt nummer» er et type telefonnummer hvor det er mottakeren av oppringingen som betaler for samtalen, og er i 800-nummerserien, se Nasjonal kommunikasjonsyndighet, «Alle nummerserier for norske telefonnummer» (*Nasjonal kommunikasjonsmyndighet*) <https://www.nkom.no/telefoni-og-telefonnummer/telefonnummer-og-den-norske-nummerplan/alle-nummerserier-for-norske-telefonnumre#8_og_12sifrede_nummer> sammenholdt med Wikipedia, «Alfanummer» (*Wikipedia*, sist redigert 30. desember 2015) <https://no.wikipedia.org/wiki/Alfanummer >, begge besøkt 23. mars 2023

2.[15] Videre var det å direkte overføre teletjeneste til seg selv ifølge Høyesterett å «uberettiget påvirke resultatet av en automatisert databehandling». Databedrageribestemmelsen kom derfor til anvendelse.

Nest siste gjerningsalternativ i databedrageribestemmelsen er at gjerningspersonen «disponerer over et kredittkort eller debetkort som tilhører en annen». Ordlyden oppstiller tre krav. For det første er det krav om at en «disponerer», som etter alminnelig språklig forståelse tilsier bruk. Videre må bruken være gjort med et «kredittkort eller debetkort», og ordlyden tilsier et betalingskort der det enten ytes kreditt eller der det opp imot innestående saldo foregår en kontinuerlig avregning. Deretter kan straffansvar kun ilegges om en annen enn gjerningspersonen er eier av kortet jf. «tilhører en annen».

Gjerningsalternativet ble tilføyd databedrageribestemmelsen etter vedtakelsen av den «nye» straffeloven i 2005. Forarbeidet gir uttrykk for at tilføyelsen, i lys av at gjerningsalternativet representerer et av de mest praktiske tilfellene av databedrageri, gjør loven mer «tilgjengelig og informativ» jf. Ot.prp. nr.22 (2008-2009) side 326. Av samme sted fremgår det at straffansvar forutsetter at bruken er uberettiget. De tilfeller hvor gjerningspersonen er gitt tillatelse til å disponere over betalingskortet faller dermed utenfor databedrageribestemmelsen.

Et eksempel på anvendelse av tredje gjerningsalternativ fremgår av tingrettens behandling ved LA-2018-53831, *Uno X-dommen*.[16] Lagmannsrettens ankebehandling bortfalt som følge av at forfølgning var besluttet frafalt av kompetent myndighet, og retten avsa frifinnelsesdom. I tingretten ble derimot den tiltalte domfelt for overtredelse av databedrageribestemmelsen for å ha «benyttet et Visa-kort tilhørende en annen» til å tilegne seg til sammen omtrent 18 000 liter diesel for til sammen nesten 200 000 kroner fra ulike Uno-X bensinstasjoner. Bensinstasjonene var selvbetjente. Betalingskortet ble brukt overfor en maskin, og medførte at tiltaltes handling «uberettiget påvirket en automatisert databehandling». Tingretten domfelte derfor etter strl. § 371 bokstav b.

Dersom misbruk av bankkort består av direkte uttak av kontanter eller varer ved en automatisert databehandling tilsier imidlertid forarbeidene at handlingen skal subsumeres etter tyveribestemmelsen, se Ot.prp. nr. 22 (2008-2009) s. 476 med henvisning til Ot.prp. nr.

[15] Lov 22. mai 1902 nr. 10 (straffeloven)
[16] TNETE-2017-94511

35 (1986-1987) s. 26. Det er derfor grunn til å både stille spørsmål ved tingrettens lovanvendelse i *Uno X-dommen* og foreta en nærmere vurdering av en slik handling opp imot databedrageri- og tyveribestemmelsen. Dette blir behandlet i henholdsvis kapittel 7 og 8.

En praktisk situasjon som kan aktualisere anvendelse av tredje gjerningsalternativ er følgende: Person A er av person B blitt gitt et betalingskort tilhørende B, med en instruks om å kjøpe vare X til B via netthandel. A kjøper i stedet vare Y til seg selv. I et slikt tilfelle er det i utgangspunktet gitt tillatelse til å disponere over koret, og forarbeidets krav om «uberettiget» bruk tilsier dermed at saksforholdet faller utenfor databedrageribestemmelsen jf. Ot.prp. nr. 22 (2008-2009) s. 326. Ved et slikt saksforhold bærer gjerningspersonens handling preg av illojalitet, og det er derfor nærliggende å vurdere straffansvar etter strl. § 324 om underslag med B som fornærmede. Imidlertid er det ikke gitt tillatelse til den aktuelle disposisjonen som A foretar. En kan derfor stille spørsmål om A kan anses å ha begått databedrageri overfor nettbutikken og/eller utstederen av betalingskortet for bruken av Bs kort til å kjøpe varen Y til seg selv. Både nettbutikken og utstederen oppfyller vilkåret om at databedrageriet må være utført mot «noen», A «disponerer» over et «[betalings]kort som tilhører en annen» i strid med gitt instruks, handlingen «volder» «tap eller fare for tap» hos nettbutikken og/eller kortutstederen, og betalingsprosessen er en «automatisert databehandling». Den beskrevne situasjonen er dermed egnet til å illustrere anvendelse av databedrageribestemmelsens tredje gjerningsalternativ.

Fjerde og siste gjerningsalternativ er den såkalte sekkebestemmelsen om å «på annen måte» uberettiget påvirke resultatet av en automatisert databehandling. Ordlyden innebærer at databedrageribestemmelsen har en ikke-uttømmende gjerningsbeskrivelse. Det er dermed åpnet for at det kan være fremgangsmåter som av sin art utgjør å «uberettiget påvirke resultatet av en automatisert databehandling», men som ikke konkret er forutsett av lovgiver. Følgelig vil det avgjørende i slik tilfeller være om gjerningspersonens handling forleder en datamaskin ved at den «uberettiget påvirker resultatet av en automatisert databehandling». Matningsdal uttaler at dette alternativet omfatter for eksempel tilføyelse av nye eller sletting av lagrede opplysninger.[17]

[17] Matningsdal (2017) s. 986.

2.3 Alminnelig bedrageri

Straffeloven § 371 bokstav a:

> *«Med bot eller fengsel inntil 2 år straffes den som med forsett om å skaffe seg eller andre en uberettiget vinning […] fremkaller, styrker eller utnytter en villfarelse og derved rettsstridig forleder noen til å gjøre eller unnlate noe som volder tap eller fare for tap for noen.»*

2.3.1 «fremkaller, styrker eller utnytter» en «villfarelse»

Inngangsvilkåret ved alminnelig bedrageri er at det må foreligge en «villfarelse». Ordlyden tilsier en uriktig eller usann oppfatning. I juridisk teori er det gitt uttrykk for at det er irrelevant for anvendelsen av straffebudet hvorvidt villfarelsen er uvitenhet eller om det er spesifikke forestillinger om et konkret, men uriktig faktum.[18]

Deretter er det krav om at den aktuelle villfarelsen er noe gjerningspersonen «fremkaller, styrker eller utnytter». Ordlyden «eller» innebærer at det er alternative vilkår. At gjerningspersonen «fremkaller» en villfarelse tilsier at den uriktige eller usanne oppfatningen ikke allerede var dannet i tankene til vedkommende som forledes, men at gjerningspersonen skaper den – enten ved ord, handling eller unnlatelse. Det er en årsakssammenheng mellom gjerningspersonens opptreden og villfarelsen som skapes. Ordlyden «styrker» og «utnytter» tilsier at villfarelsen allerede er dannet hos den som blir forledet, og at gjerningspersonen ikke korrigerer villfarelsen. Hen opptrer heller slik at vedkommende blir mer overbevist eller gjerningspersonen velger å dra fordel av villfarelsen. Felles for «fremkaller» og «styrker» er at ordlyden tilsier et krav om at gjerningspersonens opptreden er årsak til vedkommendes (grad av) villfarelse.

Vilkårene om «villfarelse» og at denne må blir «fremkalt, styrket eller utnyttet» tilsvarer innholdet i databedrageribestemmelsens alternative gjerningsbeskrivelser. Å «bruke uriktig eller ufullstendig opplysning», «endrer data eller datasystem», «disponere over kredittkort eller debetkort som tilhører en annen» eller «på annen måte» uberettiget påvirker, innebærer

[18] Matningsdal (2017) s. 975

alle at gjerningspersonen enten skaper eller utnytter en feilopplysning i et automatisk datasystem.

2.3.2 Årsakssammenheng

Det tredje kravet ved den alminnelige bedrageribestemmelsen er at gjerningspersonens fremkallelse, styrkelse eller utnyttelse av en villfarelse må være årsaken til at gjerningspersonen «rettsstridig forleder noen til å gjøre eller unnlate noe som volder tap eller fare for tap» jf. ordlyden «derved». Etter en alminnelig språklig forståelse forutsetter det at man gjør en konkret vurdering av først om en annen er blitt «forlede[t]» av gjerningspersonens handling eller unnlatelse, deretter om dette har medført at vedkommende «gjør eller unnlater[r] noe».

Ordlyden «forlede» tilsier at en annen, i lys av den aktuelle situasjonen, blir lurt til å handle eller unnlate å gjøre noe, og at denne handlemåten kan betegnes som galt. Vilkåret, og dermed anvendelse av den alminnelige bedrageribestemmelsen, forutsetter derfor et element av en sosial situasjon i hendelsesforløpet.[19] Til sist må en også vurdere om det er årsakssammenheng mellom vedkommendes opptreden og at det er oppstått «tap eller fare for tap», jf. ordlyden «volder». Det er dermed to krav om årsakssammenheng ved alminnelige bedrageri.

Dersom gjerningspersonen foretar en aktiv handling vil det sjeldent være tvil om årsakssammenheng.[20] Hvis gjerningspersonen i stedet opptrer passivt, for eksempel ved at hen unnlater å gi opplysninger hen er forpliktet å gi, poengterer juridisk teori at motparten vil trekke slutninger av gjerningspersonens taushet[21]. Passivitet vil derfor kunne oppfylle kravet om årsakssammenheng og oppfylle kravet om å «forlede» noen.

Gjerningspersonens forsett må også dekke at den forledede foretar eller unnlater noe om skaper (fare for) tap, jf. strl. § 22 første ledd.

[19] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet* (Bergen, Fagbokforlaget 2016) s. 118
[20] Matningsdal (2017) s. 976
[21] Ibid.

2.3.3 Rettsstrids-reservasjon

Neste vilkår er at forledelsen må være fremkalt som følge av at gjerningspersonen har opptrådt «rettsstridig». Ordlyden oppstiller en rettslig avgrensning av hvilke forledelser som medfører straffansvar. Samfunnets økonomiske system er avhengig av adgangen til å forhandle frem og markedsføre avtaler, og rettsstridsreservasjonen er derfor en nødvendig avgrensning.[22] Reservasjonen omfatter derfor også forledelse som følge av taushet. Vurderingstemaet vil da være om motparten hadde en berettiget forventning om den fortiede opplysningen, og det er videre strengere krav for at en fortielse skal anses rettsstridig.[23]

Stortingspensjon-dommen, Rt. 2012 s. 622, er i juridisk teori fremhevet som sentral for rettsstridsvurderingen.[24] I dommen hadde den tiltalte oppnådd en uberettiget utbetaling som følge av å ikke ha gitt tilstrekkelige opplysninger, og ble dømt for overtredelse av den alminnelige bedrageribestemmelsen. I rettsstridsdrøftelsen uttalte Høyesterett at det for vurderingen er «avgjørende om gjerningspersonen har opptrådt i strid med redelighet og god tro – om han har opptrådt utilbørlig» jf. avsnitt 30. Og videre, at lovgivers valg om rettsstridsreservasjon innebærer at grensen for hva som er straffbart etter alminnelig rettsoppfatning er overlatt til domstolene, jf. avsnitt 30.

Rettsstridsvurderingen tar altså utgangspunkt i hvorvidt gjerningspersonen har opptrådt i strid med redelighet og god tro, og innebærer en moralsk dom over handlingen.[25] Vurderingen inneholder mange av de samme momentene som ved vurderingen etter avtaleloven § 33.[26] En begynner derfor med å se hen til samfunnsområdet hvor gjerningen ble begått. Deretter er følgende momenter sentrale for vurderingen: Om tiltaltes handlemåte i lys av saksområdet er å anse som akseptabel, om det er veiledende lovregulering på området og styrkeforholdet mellom partene.[27] Anvendelse av strl. § 371 bokstav a innebærer ileggelse av straffansvar. Terskelen for å ha handlet i strid med redelighet og god tro vil derfor være strengere enn ved en vurdering på privatrettens område. [28]

[22] Magnus Matningsdal ved Norsk lovkommentar note 2322 til § 371 bokstav a hos Rettsdata
[23] Ibid.
[24] Se for eksempel Matningsdal (2017) s. 978 og Erling Johannes Husabø ved Karon-lovkommentar, note 7 til strl. § 371 bokstav a hos Lovdata
[25] Matningsdal (2017) s. 977
[26] Erling Johannes Husabø ved Karnov-lovkommentar, note 7 til strl. § 371 bokstav a hos Lovdata
[27] Ibid.
[28] Ibid.

2.3.4 «tap eller fare for tap for noen»

Vilkåret «tap eller fare for tap for noen» er lik taps-vilkåret ved databedrageribestemmelsen, og jeg viser til tolkningen foretatt ved databedrageribestemmelsen.[29] Tidligere var tapsvilkåret ved den alminnelige bedrageribestemmelsen avgrenset ved at ordlyden tilsa at den som led tap måtte være den samme som ble forledet. Dette ble imidlertid endret slik at straffansvar ved den alminnelig bedrageribestemmelsen, slik som ved databedrageribestemmelsen, også omfatter de tilfeller der tapet rammer en tredjeperson, jf. Ot.prp. nr. 22 (2008-2009) s. 326.

Minimumskravet om at det må være frembragt et potensiale for tap er felles for bedrageritypene, jf. «fare for tap». For alminnelig bedrageri vil tidspunktet det har oppstått «fare for tap» også utgjøre fullbyrdelsestidspunktet for overtredelsen av gjerningsbeskrivelsen. Tilsvarende gjelder ved databedrageribestemmelsen. Der må fullbyrdelsestidspunktet imidlertid også sees i sammenheng med vilkåret om å «påvirke et resultat», og videre at dette innebærer et krav om at gjerningspersonens handling har «frembragt et resultat» jf. Rt. 1991 s. 532 på s. 534. Tilsvarende fremgår av ordlyden til den alminnelige bedrageribestemmelsen ved at det er krav om at gjerningspersonens forledelse må føre til at noen «gjør eller unnlater» noe som så minimum medfører en «fare for tap».

2.3.5 Sammenligning med databedrageri

I LG-2009-9070-2 var en kvinne tiltalt etter strl. 1902 § 270 første ledd nr. 2 jf. annet ledd for å ha benyttet «stjålne, falske eller ugyldige kredittkort/kredittkortinformasjon til å forelde ansatte ved [SAS] eller personer som handlet på vegne av selskapet eller ved automatisk databehandling […]». Tiltalen viste til databedrageribestemmelsen i den dagjeldende straffeloven, og kjernen av straffebudet var forledelse av en automatisert databehanding slik som ved dagens straffebud. Det er derfor oppsiktsvekkende at grunnlaget for tiltalen beskriver forledelse av personer – som heller et vilkår ved alminnelig bedrageri. Lagmannsrettens behandling fikk frem at tiltalte hadde forledet en «automatisert databehandling» og korrigerte dermed den upresise tiltalebeslutningen. Sakens tiltalebeslutning illustrerer at det kan være utfordrende å differensiere mellom alminnelig bedrageri og databedrageri.

Videre er det lett å falle i fella om at ethvert teknologisk element gjør et bedrageri til et databedrageri. HR-2022-2468-A viser at selv om fremgangsmåten ved et bedrageri er

[29] Se delkapittel 2.4.2

avhengig av at gjerningspersonen misbruker teknologi, så er ikke det alene tilstrekkelig for å forfølge handlingen som databedrageri. Bedrageriet var utført blant annet ved urettmessig innlogging i nettbankkonto og misbruk av BankID – kriminelle handlinger som er blitt relativt vanlig.[30] Ettersom de tiltalte hadde «forledet» personer til å oppgi sensitiv informasjon som var nødvendig for at gjerningspersonen så misbrukte BankIDen deres, ble de domfelt for alminnelig bedrageri.

Likheter mellom bedrageribestemmelsene er blitt kommentert fortløpende, men det interessante for oppgavens problemstilling er hvordan bedrageritypene skiller seg fra hverandre. En sammenligning av bestemmelsene viser at elementet «lureri», som i utgangspunktet er et fellestrekk, også byr på flere forskjeller mellom bestemmelsene.

Ved alminnelig bedrageri er det et tydelig sosialt aspekt ved gjerningspersonens handling. Under forutsetningen om at forsettkravet er oppfylt, må det skje en interaksjon med et eller flere mennesker jf. «forleder noen». Det er en tydelig karakteristikk ved handlingene som faller inn under strl. § 371 bokstav a. Ved databedrageribestemmelsen er imidlertid gjerningspersonens list rettet mot en «automatisert databehandling», og ikke en person. Midlene for forledelse ved bedrageritypene er dermed forskjellig. I motsetning til alminnelige bedrageri kan handlinger som faller inn under databedrageribestemmelsen karakteriseres ved totalt fravær av menneskelig interaksjon. Spørsmålet som da oppstår er hvordan en skal behandle de tilfellene der gjerningspersonen feilaktig tror at hens list er fri for menneskelig interaksjon, men i realiteten innebærer at hen «forleder noen».

Sunde eksemplifiserer og behandler et slikt tilfelle. Gjerningspersonen har i en nettbasert bestillingsprosess brukt en annens betalingskort og har handlet med et forsett om å «uberettiget påvirke en automatisert databehandling». I realiteten er det imidlertid mennesker som utfører kontroll av bestillingene. Førte tanke kan da være at gjerningsbeskrivelsene i § 371 ikke er oppfylt. Gjerningspersonen har ikke et forsett som dekker å «forlede noen» jf. bokstav a, og gjerningspersonen har heller ikke forsettlig «uberettiget påvirket en automatisert databehandling jf. bokstav b. Imidlertid, slik Sunde poengterer, er vilkåret ved databedrageri at «noen» påføres et tap. Nettbutikken vil motta betaling for bestillingen, og det er betalingskortutstederen som lider tap. Betalingstransaksjonen utgjør overfor kortutstederen en

[30] Victoria Marie Nordahl; Kjetil Samuelsen, «Kunder svindlet fra bankens eget telefonnummer: - Simpelt gjort» (NRK, 13. mai 2022) <https://www.nrk.no/sorlandet/kunder-svindlet-fra-bankens-eget-telefonnummer-1.15961171> besøkt 24. mars 2023

handling fri for menneskelig interaksjon, og deres tap er dermed skjedd ved at gjerningspersonen «uberettiget påvirker en automatisert databehandling». Sunde mener derfor at slike tilfeller i utgangspunktet skal behandles som databedrageri.[31] Det tilsier at ved det tidligere eksemplifiserte tilfellet om person A som ved nettkjøp handler utover instruksen gitt av B, så skal As handling anses som databedrageri overfor kortutstederen.[32]

At det kun er en dataprosess som føres bak lyset ved databedrageribestemmelsen er en annen forskjell ved bestemmelsenes «lureri»-element. Ordlyden i § 371 bokstav a om «forledelse» tilsier som nevnt at en annen person blir lurt til å ut ifra situasjonen handle «galt». Ved bokstav b fokuserer derimot ordlyden kun på handlingene til gjerningspersonen, og det er kun hen som handler «galt» jf. ordlyden «den som […] uberettiget påvirker». Dette understreker at handlinger som faller inn under databedrageribestemmelsen er særegne ved at den eneste personen involvert er gjerningspersonen.

Straffeloven § 371 bokstav a er reservert for tilfellene som medfører at gjerningspersonen «rettsstridig» forleder noen. En tilsvarende avgrensning av anvendelsesområde finner en i databedrageribestemmelsen. Der er kravet at gjerningspersonens handling må «uberettiget» påvirke den automatiserte databehandling. Som nevnt fremgår det av Ot.prp. nr. 22 (2008-2009) på side 22 at dette utgjør en rettsstridsreservasjon. En likhet ved de to bestemmelsene er dermed at det må gjøres en rettsstridsvurdering, og at dette innebærer en konkret vurdering av om gjerningspersonens handlemåte er innenfor hva som er å anse om akseptabel atferd på det aktuelle saksområdet. Innad likheten ligger imidlertid også en forskjell. Rettsstrids-reservasjonen ved den alminnelige bedrageribestemmelsen har en hensikt om å gi slingringsmonn til å kunne inngå fordelaktige avtaler med en annen person. På grunn av manglende menneskelig interaksjon ved databedrageri er det derimot vanskelig å tillegge tilvarende hensikt ved databedrageribestemmelsens rettsstridsreservasjon. Vurderingene vil derfor ikke kunne foretas etter helt like vurderingsmomenter.

Samlet: Det som karakteriserer handlinger og hendelsesforløp som faller inn under databedrageribestemmelsen er at gjerningspersonens handlinger retter seg mot et datasystem fri for menneskelig informasjonsbehandling eller -kontrollfunksjon.

[31] Sunde (2016) s. 127
[32] Se delkapittel 2.2.3, om databedrageribestemmelsens tredje gjerningsalternativ

Spørsmålet som da gjenstår er hvordan dette fungerer i praksis. En kan se for seg at en arbeidsgiver instruerer arbeidstakeren om, via nettbank, å gjennomføre en rekke betalinger til person X – noe som innebærer en «automatisert databehandling». Arbeidstakeren er imidlertid av den uærlige typen, og har allerede ved tidspunktet for instruksen bestemt seg for at betalingene skal gå til hen selv.[33] De «uriktige opplysningene» som anvendes ved betalingen kan innebære at handlingen faller inn under databedrageribestemmelsen. Samtidig kan en vurdere situasjonen til at arbeidstakerens uærlige bekreftelse på instrukstidspunkter er å «styrke» eller «utnytte» en «villfarelse» hos arbeidsgiveren. Dette «forleder» så arbeidsgiveren til å «unnlate» å håndtere situasjonen på en annen måte», jf. strl. § 371 bokstav a.

Den foreløpige slutningen om databedrageribestemmelsen anvendelsesområde opp imot alminnelig bedrageri er ikke nødvendigvis tilstrekkelig for å ta stilling til en slik problemstilling. Relevant er også rettspraksis som behandler tvil om valg av de to bestemmelsene. Kapittel 4, 5 og 6 drøfter rettspraksis som er interessant for spørsmålet av hva som karakteriserer de handlinger som faller inn under de to bedrageribestemmelsene.

2.4 Tyveri

Straffeloven § 321:

> *«For tyveri straffes den som tar en gjenstand som tilhører en annen, med forsett om å skaffe seg eller andre en uberettiget vinning ved å selge, forbruke eller på annen måte tilegne seg den.»*

2.4.1 «tar»

Første vilkår ved tyveribestemmelsen er «tar», og ordlyden tilsier at noe fjernes fra dens plassering. Den tidligere ordlyden var «borttar», og allmenn juridisk oppfatning var at vilkårets ordlyd innebar et krav om en besittelsesforrykkelse fra besitter til gjerningspersonen.[34] Endringen fra «borttar» til «tar» innebar imidlertid ikke en

[33] Dette eksempelet skiller seg fra tidligere situasjon med person A som anvender betalingskortet til person B, ettersom det her ikke er en kortusteder som lider tap som følge av As disposisjon. Se delkapittel 2.2.3 om eksemplifisering til databedrageribestemmelsens tredje gjerningsalternativ.
[34] Se for eksempel Johs. Andenæs, *Spesiell strafferett og formuesforbrytelsene* (samlet utgave ved Kjell V. Andorsen, Oslo, Universitetsforlaget 2008*)* s. 313-314, og Matningsdal (2017) s. 813 og (2021) s. 322-323

realitetsendring jf. Ot.prp. nr. 22 (2008-2009) s. 451, og den fastlagte forståelsen av vilkåret i både eldre rettspraksis og juridisk teori gjelder fremdeles. Gjerningspersonens handling må dermed krenke besitterens rådighet over gjenstanden. En besittelsesløs gjenstand kan ikke oppfylle vilkåret, og annen lovgivning vil i så tilfelle komme til anvendelse.[35]

2.4.2 «gjenstand»

Neste vilkår er at gjerningspersonen må ta «en gjenstand», og ordlyden tilsier et fysisk objekt. Konteksten «tar» tilsier videre at tyveribestemmelsen er avgrenset til å omfatte ting, og ordlyden «gjenstand» tilsier derfor løsøre. Anvendelsesområdet er imidlertid videre som følge av legaldefinisjonen i strl. § 12 om at med «gjenstand» i straffeloven «menes også elektrisk energi eller annen energi».

2.4.3 «tilhører en annen»

Ordlyden «tilhører en annen» tilsier at gjenstanden ikke kan være eierløs og at en annen person enn gjerningspersonen har eierskap over tingen. Det fremgår av Ot.prp. nr. 22 (2008-2009) s. 451 at den tidligere ordlyden presiserte at også gjenstander som kun delvis tilhører en annen er omfattet av bestemmelsen. Ordlydsendringen innebar imidlertid ikke en realitetsendring jf. samme sted. En gjenstand hvor eierforholdet er sameie, og hvor gjerningspersonen ikke har gjenstanden i sin besittelse, kan dermed også bli urettmessig borttatt slik at tyveribestemmelsen kommer til anvendelse.

Vilkåret «tilhører en annen» innebærer ikke et krav om at vedkommende som får besittelsen krenket og skadelidende er den samme. En låntaker av en gjenstand kan dermed være den som umiddelbart får en midlertidig besittelse krenket, men det er eieren som overordnet er den skadelidende.[36] Tilsvarende skille mellom skadelidende og hvem den kriminelle handlingen retter seg mot er å finne i databedrageribestemmelsen. Der er det vilkår om at «noen» blir utsatt for tap eller fare for tap, og som nevnt betyr det at: Det er ikke krav om at eieren av den automatiserte databehandlingen, som ved databedrageri blir ført bak lyset, også er den som blir utsatt for (potensialet for) et økonomisk tap. For eksempel kan en kortutsteder benytte seg av elektronisk betalingsløsning levert av en tredjepart, og i slikt tilfelle vil den

[35] Matningsdal (2017) s. 812
[36] Se for eksempel Matningsdal (2021) s. 322

databedragerske handlingen bli utført overfor tredjeparten. Det tilsvarer en låntaker som opplever besittelseskrenkelsen. Derimot er det kortutstederen som sørger for det økonomiske oppgjøret og dermed lider tap, noe som tilsvarer eieren som den skadelidende ved at gjenstanden «tilhører» hen.

2.4.4 Uberettiget vinning- og tilegnelsesforsett

Til sist må gjerningspersonen ha «forsett om å skaffe seg eller andre en uberettiget vinning» «ved å selge, forbruke eller på annen måte tilegne seg» gjenstanden. Vilkåret om «forsett om […] uberettiget vinning» er en likhet med databedrageribestemmelsen. For vilkårets innhold viser jeg til innledende felles tolkning for de tre bestemmelsene.[37]

Ordlyden «eller på annen måte tilegne seg den» tilsier at det avgjørende er om gjerningspersonen handler med forsett om å «tilegne» seg gjenstanden og slik oppnår en uberettiget vinning. Kontekstuelt er oppramsingen «selge, forbruke» eksempler på slik tilegnelse. Tilsvarende fremgår av Ot.prp. nr. 22 (2008-2009) s. 451. Det innebærer dermed en avgrensning mot tilfeller der en gjenstand borttas kun for ulovlig bruk for så å bli levert tilbake. Tilegnelsen innebærer å gjøre eller bruke tingen som sin egen, det er dermed en krenkelse av eierens eiendomsrett. Vilkåret om tilegnelse-forsett gir derfor uttrykk for straffebudets formål om vern av eiendomsretten.

2.4.5 Sammenligning med databedrageri

Likhetene er kommentert fortløpende, og sammenligningen behandler derfor forskjellene mellom databedrageri- og tyveribestemmelsen.

I motsetning til tyveribestemmelsen har ikke databedrageribestemmelsen et vilkår om tilegnelse-forsett. Dersom en gjerningsperson utfører et databedrageri for å få besittelsen av en gjenstand, men med en plan om å levere gjenstanden tilbake etter den uberettigede vinningen som oppnås ved eget eller en annens bruk, vil databedrageribestemmelsen fremdeles være anvendelig. Et hverdagslig eksempel er leie av bilhenger. Ved å manipulere et elektronisk utleiesystem hvor leieavtalen og utlevering av bilhengeren skjer ved en automatisert databehandling jf. strl. § 371 bokstav b andre gjerningsalternativ, oppnår

[37] Se delkapittel 2.3

gjerningspersonen lån av bilhenger. Gjerningspersonen skal levere hengeren tilbake, og handlingen er gjort fordi vedkommende ikke ønsker betale for bruken. Det foreligger dermed ikke tilegnelse-forsett.

Den beskrevne handlingen krenker ikke hensynene beskyttet ved tyveribestemmelsen, men krenker databedrageribestemmelsens hensyn. Tyveribestemmelsen er plassert i straffeloven kapittel 27 om vinningslovbrudd og lignende krenkelse av eiendomsretten. Databedrageribestemmelsen er derimot å finne i kapittel 30 om økonomisk kriminalitet med svikaktig karakter. Strl. § 371 bokstav b er dermed ikke ment å være en beskyttelse av eiendomsretten, men er i stedet ment å ramme svikaktige handlinger som krenker hensynene til datasikkerhet.[38] Databedrageri som ved bilhenger-eksempelet krenker tilliten til datasikkerheten ved moderne betalings- og avtalesystem – og i videre forstand, moderne handel. Hensynene blir krenket allerede ved den uberettigede påvirkningen av utleiesystemets automatiserte databehandling. Det er dermed ikke behov for tilegnelse-forsett for å påvise krenkelse av hensynene som beskyttes ved databedrageribestemmelsen.

En annen forskjell mellom bestemmelsene er at tyveribestemmelsens ordlyd fokuserer på gjerningspersonens fysiske handling. Vilkårene «tar» og «gjenstand» innebærer en avgrensning av hvordan gjerningspersonen kan krenke den beskyttede interessen.[39] Det avgjørende ved databedrageribestemmelsen er derimot at gjerningspersonen «uberettiget påvirker en automatisert databehandling». Dette kommer til uttrykk ved flere gjerningsalternativer, sekkevilkåret «på annen måte» og at den uberettigede påvirkningen er et fellesvilkår for gjerningsalternativene. *Hvordan* gjerningspersonen oppnår den uberettigede påvirkningen er ikke viktig. Databedrageribestemmelsen har dermed ikke en tilsvarende handlingsavgrensning for overtredelse av straffebudet som tyveribestemmelsen. Spørsmålet er imidlertid hvilken betydning dette har dersom begge hensyn blir krenket.

En illustrerende problematisering finner en blant nye, kreative butikkløsninger. Ved Amazon Fresh-butikkene er konseptet følgende: Kunden skanner egen Amazon-konto idet hen går inn i butikken. Deretter plukker vedkommende de varene hen ønsker, og forlater så butikken. Handleturen er fri fra både skanning av varer og en betalingstransaksjon der kunden anvender en kortmaskin i butikken. Varene er i stedet blitt registrert uttatt ved kundens konto, blant

[38] Se Ot.prp. nr. 22 (2008–2009) s. 62 og Sunde (2019) s. 14
[39] Vilkåret vil for eksempel også være oppfylt der gjerningspersonen bruker et dyr til å bortta og oppnå besittelsen av en gjenstand.

annet ved bruk av kameraovervåking, og blir belastet Amazon-kontoen idet kunden forlater butikken. Men, hva skjer om kunden, i stedet for å skanne egen Amazon-konto, skanner en konto tilhørende en annen? Overfor butikken oppstår det en besittelseskrenkelse ved borttakelsen av varene. Samtidig har gjerningspersonen lurt Amazons automatiserte databehandling til å belaste en annens Amazon-konto. Med tanke på subsumsjonsvalg kan en da stille spørsmål om det mest fremtredende ved hendelsesforløpet og gjerningspersonens handling er besittelseskrenkelsene ved borttakelsen av varene, eller krenkelsen av datasikkerhet ved at vedkommende lurer dataprogrammet som sørger for belastning for vareuttaket.

Subsumsjonstvil som kan oppstå mellom krenkelsen av eiendomsretten og datasikkerheten blir problematisert og behandlet nærmere under kapittel 7. Med bakgrunn i høyesterettspraksis stilles spørsmålet hvorvidt borttakelse av kontanter eller ting fra en automat skal bedømmes som tyveri eller databedrageri.

2.5 Oppsummering

Sammenligningen av gjerningsbeskrivelsene er et nyttig teoretisk utgangspunkt i kartleggingen av hva som karakteriserer de handlinger som faller inn under de tre bestemmelsene. Et helhetlig analytisk grunnlag for å besvare den overordnede problemstillinger forutsetter imidlertid også en vurdering av hvordan bestemmelsene er anvendt av domstolen. Kapittel 4-7 behandler derfor domstolenes drøftelse av hvilken av bestemmelsene saksforholdet faller inn under, eller saker hvor en kan problematisere hvorvidt retten burde foretatt en slik drøftelse.

Det er mangfoldige, kreative måter en kan utnytte teknologi til å begå kriminalitet. Kapittel 3 presenterer tre situasjoner hvor gjerningspersonens anvendelse av teknologi er egnet til å illustrere spenningen mellom de tre straffebudene. Subsumsjon av lovbruddene forutsetter imidlertid at det først tas stilling til den overordnede problemstillingen, og subsumsjonene gjøres derfor i kapittel 8.

3 Moderne lovbrudd

3.1 Uberettiget kontantuttak fra automat med bankkort som tilhører en annen

En vanlig hverdagsbekymring er å bli frastjålet bankkortet sitt. Ofte vil borttakelsen av et bankkort oppfylle vilkårene for tyveri, jf. strl. § 321. Det er derimot sjeldent borttakelsen som er årsaken til bekymringen. Redselen er knyttet til muligheten for misbruk av bankkortet som oppstår ved uberettiget borttakelse. Misbruken kan for eksempel være uberettiget kontantuttak fra automat – en situasjon som kan skape subsumsjonstvil mellom tyveri- og databedrageribestemmelsen.

Årsaken til slik subsumsjonstvil begynner med Rt. 1982 s. 1816. I dommen konkluderte Høyesterett med at der gjerningspersonen gjør uttak fra en minibankautomat slik at det medfører overtrekk på egen konto så har vedkommende som følge av en uberettiget borttakelse av kontanter begått tyveri overfor banken.[40] Først tenker en kanskje at Høyesteretts subsumsjonsvalg kan forklares ved at databedrageribestemmelsen ikke ble vedtatt før i 1987.[41] Det fremgår imidlertid av forarbeid til databedrageribestemmelsen at Høyesteretts avgjørelse skal bestå, og videre at «[m]isbruk av bankkort til direkte uttak skal derimot straffes som tyveri».[42] Forarbeidsuttalelsen tilsier at ethvert uberettiget kontantuttak utgjør brudd på tyveribestemmelsen.

Derimot, da 1982-kjennelsen ble avsagt og databedrageribestemmelsen vedtatt, var det hverken etablert et felles elektronisk betalingssystem for bankaktørene eller mulighet for umiddelbar kontroll av hvorvidt en har dekning på konto. Dette var teknologiske nyvinninger først ved begynnelsen av 1990-tallet.[43] Saksforholdet som førte til overtredelse av tyveribestemmelsen i 1982 ville dermed trolig ikke vært mulig bare ti år senere. Siden har det vært alt annet enn bremser på den teknologiske utviklingen. En kan derfor stille spørsmål ved hvorvidt Høyesteretts subsumsjon og etterfølgende forarbeidsuttalelser har passert siste

[40] Rt. 1982 s. 1816 s. 1817-1818, se også Høyesteretts redegjørelse for 1982-kjennelsen i Rt. 1990 s. 17
[41] Inger Marie Sunde, *Datakrimretten i «fugleperspektiv»* (Tidsskrift for strafferett, 19(2), 129-147) s. 10 i nedlastet versjon
[42] Ot.prp. nr. 35 (1986-1987) s. 26
[43] Ellen Katrine Nyhus, «BankAxept» (*Store norske leksikon*, 6. juli 2021) < https://snl.no/BankAxept > besøkt 02. mars 2023

forbruksdag, og at uberettiget kontantuttak i stedet bør falle inn under databedrageribestemmelsen.

Spørsmålet ble imidlertid tatt stilling til i lovforarbeid Ot.prp. nr. 22 (2008-200) s. 325 ved innføring av någjeldende tredje gjerningsalternativ om betalingskort i databedrageribestemmelsen, og lovgiver holdt fast ved anvendelse av tyveribestemmelsen. Derimot igjen, dette er nå mer enn ti år siden. Det er derfor interessant å drøfte under delkapittel 8.2 hvordan uberettiget uttak av kontanter med bankkort som tilhører en annen skal, eventuelt bør, subsumeres.

3.2 Uberettiget tilegnelse av strøm

Tradisjonelt blir uberettiget tilegnelse av strøm subsumert under tyveribestemmelsen.[44] Vilkåret «gjenstand» jf. § 321 er legaldefinert ved strl. § 12 til å «også mene elektrisk energi eller annen energi». Legaldefinisjonen ble vedtatt etter at uberettiget tilegnelse av strøm ved tilkobling til strømnettet utenom strømmåleren i flere år hadde falt inn under tyveribestemmelsen i rettspraksis.[45] Et eksempel er Rt. 2009 s. 683 og Høyesteretts behandling av straffutmåling etter domfellelse for grovt tyveri av strøm. Den domfelte hadde borttatt elektrisk kraft fra strømnettet utenom strømmåler jf. faktumbeskrivelse i tilhørende LE-2009-34828.[46] Felles for saksforholdene behandlet i rettspraksis er at tilegnelsen av strømmen har skjedd ved tilkobling til strømnettet utenom strømmåler.

I nyere tid er det imidlertid vært en utvikling innenfor registrering og betaling av strømforbruk. I 2011 ble det forskriftsfestet at alt strømforbruk fra og med 1. januar 2019 skal bli registrert med en AMS-måler.[47] AMS står for «avanserte måle- og styringssystemer» og gjør at innrapportering av strømforbruk ikke lenger skjer ved manuell avlesing. I stedet er det en automatisk prosess som både registrerer og rapporterer strømforbruket til det aktuelle strømselskapet.[48]

---

[44] Andenæs (2008) s. 312
[45] Se NOU 2002: 4 Ny straffelov, se side 209, og Ot.prp. nr. 90 (2003-2004), se side 409. Se også Matningsdal (*Straffeloven: Kommentarutgave* 2017) side 810
[46]
[47] Se FOR-2011-06-24-726 *Forskrift om endring i forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester*
[48] NVE, «AMS» (*Norges vassdrag- og energidirektorat*, 27. oktober 2015) <https://www.nve.no/reguleringsmyndigheten/kunde/nett/ams/> besøkt 31. januar 2023

Den nye systemet for rapportering innebærer en automatisert databehandling ved datasystemet i AMS-målerne. Videre er det blitt rapportert at slike målere kan bli «hacket». Det er mulig å bryte seg gjennom datasystemets sikkerhetsmur og dermed gjøre endringer ved datasystemet.[49] En gjerningsperson kan dermed hacke en AMS-måler for å «endre på datasystemet» slik at en «uberettiget påvirker» innrapporteringen ved «automatiserte databehandling». Slik vil det innrapporterte forbruket være lavere enn det reelle forbruket, og strømkunden oppnår en uberettiget vinning samtidig som hen «derved volder» strømleverandøren «et tap».[50]

En interessant spørsmål er dermed hvordan påtalemyndigheten og domstolene vil, eller bør behandle et slikt tilfelle. Skal en falle tilbake på den tradisjonelle subsumsjonen av uberettiget tilegnelse av strøm, eller skal man vektlegge at AMS-måleren er blitt manipulert og derfor subsumere under databedrageribestemmelsen? Etter å ha tatt stilling til den overordnede problemstillingen blir spørsmålet drøftet under delkapittel 8.3.

3.3 Gjentakende tilegnelse av gratis prøveperiode til digitalt abonnement

Våren 2022 hørte jeg om et «smutthull» ved visse digitale abonnementstjenester som tilbyr en gratis prøveperiode. Ved disse er det mulig å benytte falske opplysninger, som epostadresse og mobilnummer, sammen med et midlertidig digitalt betalingskort til å registrere seg for tjenestens tilbudte gratis prøveperiode. Dette er noe en så gjentar etter hver endte gratis prøveperiode, og en behøver aldri begynne å betale for tjenesten.

En slik fremgangsmåte illustrer godt de nye kriminelle mulighetene som følger med den teknologiske utviklingen. Hvilken straffebestemmelse som kommer til anvendelse i slike tilfeller virker imidlertid ikke å ha blitt behandlet tidligere, og jeg drøfter det under delkapittel 8.4.

[49] Jannicke Nilsen, «Norske nettselskap er enige: AMS utgjør en risiko for datasikkerheten» (*Teknisk ukeblad*, 1. september 2015) <https://www.tu.no/artikler/norske-nettselskap-er-enige-ams-utgjor-en-risiko-for-datasikkerheten/275560> besøkt 31. januar 2023
[50] Leif Hamnes, «Tappet kraftselskap for 2,3 milliarder» (*E24*, 22. april 2012) <https://e24.no/teknologi/i/G1Ebmq/tappet-kraftselskap-for-23-milliarder> besøkt 31. januar 2023 for eksempel på datainnbrudd- og endring ved AMS-måler i USA

4 Teletorg: Bedrageri eller databedrageri?

4.1 Rt. 1995 s. 1704 og Rt. 1996 s. 1673

Felles for Rt. 1995 s. 1704, *Teletorg-dommen 1*, og Rt. 1996 s. 1673, *Teletorg-dommen 2*, er at de tiltalte var dømt for overtredelse av den alminnelige bedrageribestemmelsen, men at lovanvendelsen senere er problematisert i juridisk teori. Bing mfl. argumenterer for at dersom bedrageriet anses fullbyrdet «etter hvert som teleoperatørens trafikkdata ble endret som følge av gjerningsmannens oppringing til egen teletorgtjeneste», vil rett lovanvendelse heller være databedrageribestemmelsen ved straffeloven 1902 § 270 første ledd nr. 2.[51] Resonnementet er at gjerningspersonen «endrer data» hos teleoperatøren ved å ringe egen teletorgtjeneste,[52] og slik «uberettiget påvirker resultatet av en automatisert databehandling» i det tellerskrittene blir registrert og automatisk innrapportert til teleoperatøren.[53]

Ankebehandlingen ved *Teletorg-dommen 1* omfattet lovanvendelsen og straffutmålingen, og anken ved *Teletorg-dommen 2* var begrenset til straffutmålingen. Resonnement som i ettertid er presentert av Bing mfl. ble hverken anvendt eller påpekt av domstolen i noen av avgjørelsene. Det betyr at en kan stille spørsmål ved rettens subsumsjon og hvordan bedrageribestemmelsene skal anvendes.

I *Teletorg-dommen 1* var tiltalte domfelt i byretten for overtredelse av den alminnelige bedrageribestemmelsen. Han hadde opprettet to teletorglinjer som han deretter ringte inn til selv, slik at det ble registrert tellerskritt hos teletorgnummeret. Tellerskrittene resulterte så i utbetaling av teletorgnummerets fortjenesteandel fra Televerket. Det ble anket over lovanvendelsen, og domfelte anførte for Høyesterett at det på grunn av automatikken ved utbetalingen ikke forelå en «villfarelse» hos televerket, og gjerningsbeskrivelsen i den

[51] Jon Bing mfl., *Innføring i telekommunikasjonsrett* (Oslo, Cappelen Akademiske Forlag 2001) s. 294-295.
[52] Teletorg er et tjenestetilbud over telefon eller PC, og kan omfatte kjøp, salg, spill, rådgivning mm. Kunden hos det aktuelle teletorget betaler for tjenesten via telefonregningen hos teleoperatøren, og teleoperatøren sørger for utbetaling av inntektsandel til tjenesteleverandøren, se Ragnar Johnsen «teletorg» (*Store norske leksikon*, 28. september 2021) <https://snl.no/teletorg> besøkt 21. februar 2023
[53] Tellerskritt er kostnaden ved bruk av telefonitjeneste beregnet ved bruk av tellerskritt, som er takstimpulser for automatisk taksering av telefonsamtaler, se Halvor Bothner-By «tellerskritt» (*Store norske leksikon*, 29. september 2021) <https://snl.no/tellerskritt> 21. februar 2023

alminnelige bedrageribestemmelsen var dermed ikke oppfylt jf. strl. 1902 § 270 første ledd nr. 1.

Høyesteretts behandling av spørsmålet om rett lovanvendelse begynte med at førstvoterende kort tok stilling til byrettens lovanvendelse av vilkåret «villfarelse». Førstvoterende viste til byrettens beskrivelse av hvilken villfarelse som ble utnyttet, og tilføyde så at Høyesterett la til grunn at villfarelsen måtte antas å ha vært til stede hos ansatte i Televerket med kontrollansvar. Høyesterett konkluderte med enighet i byrettens lovanvendelse. Førstvoterendes kortfattethet gjør det utfordrende å vurdere rettens behandling av om det i saksforholdet forelå en «villfarelse» som så ført til «forledelse» av en eller flere personer. Imidlertid virker det ikke være der Bing mfl. mener skoen trykker ved deres problematisering av subsumsjonen.

I *Teletorg-dommen 2* var den tiltalte blitt domfelt i byretten for overtredelse av den alminnelige bedrageribestemmelsen for å ha uberettiget ringt egne teletorgnummer fra andre abonnenters telefonnumre. Dette resulterte i uberettiget utbetaling fra Televerket. Høyesteretts ankebehandling gjaldt kun straffeutmåling, og det er dermed ingen drøftelse av lovanvendelsen å ta stiling til. Dommen er imidlertid egnet til å illustrere hva som var et praktisk problem på 1990-tallet og hvordan det ble valgt pådømt i det norske rettssystemet, samtidig som subsumsjonen senere er kritisert i juridisk teori.

4.2 Et treffende subsumsjonsvalg?

Som nevnt argumenterer Bing mfl. for at overtredelse av databedrageribestemmelsen kan anses fullbyrdet «etter hvert som teleoperatørens trafikkdata ble endret som følge av gjerningsmannens oppringing til egen teletorgtjeneste». Dette tilsier at forfatterne ikke ser det nødvendig å drøfte hvorvidt ansatte ved Televerket var blitt «forledet» ved en «villfarelse», og en kan bare spekulere i hvorfor dette ikke i det minste ble drøftet av domstolen. Spørsmålet er hvilket subsumsjonsvalg som er det mest treffende.

Anvendelse av databedrageribestemmelsen krever at gjerningspersonens handling har forårsaket et «tap eller fare for tap» for «noen». Den utilsiktede kreditten som oppstod ved gjerningspersonens handling utgjør et «tap» for Televerket, og dermed «noen». Registreringen av tellerskritt er grunnlaget for senere utbetaling, og potensialet for den utilsiktede kreditten oppstår dermed i det gjerningspersonen foretar den nødvendige

oppringingen og tellerskrittene begynner å bli automatisk registrert. Det oppstår dermed en «fare for tap». Vilkårene ved databedrageribestemmelsen er oppfylt, og synspunktet om anvendelse av databedrageribestemmelsen er fullt mulig jf. strl. § 371 bokstav b.[54]

På den annen side fremgår det av forarbeid til databedrageribestemmelsen at der det i saksforholdet foreligger forledelse av en eller flere personer så skal en anvende den alminnelige bedrageribestemmelsen fremfor databedrageribestemmelsen.[55] I begge sakene mener retten at «noen» ved Televerket er blitt «forledet»,[56] og det taler for at domstolen i begge sakene gjorde det mest treffende subsumsjonsvalget.

Derimot igjen, ved *Teletorg-dommen 1* fremstår det som at det for byretten ikke var helt klart *hvem* av de ansatte ved Televerket som var blitt utsatt for en villfarelse. Ved Høyesteretts behandling måtte nemlig førstvoterende «legge til grunn» at villfarelsen knyttet til uberettiget utbetaling var «antatt å ha vært til stede hos de personer i televerket» som kunne hindret utbetalingen hadde de hatt kunnskap om de faktiske forholdene.[57] Dette er et grep Høyesterett ville unngått ved anvendelse av databedrageribestemmelsen, og slik unngått spekulering i hvorvidt alle vilkårene i gjerningsbeskrivelsen til alminnelig bedrageri faktisk var oppfylt. Det tilsier at for *Teletorg-dommen 1* ville anvendelse av databedrageribestemmelsen vært mer treffende.

For *Teletorg-dommen 2* foreligger det imidlertid ingen tvil i domspremissene om at «forledelses»-vilkåret var oppfylt, og i lys av nevnte forarbeidsuttalelse var Høyesteretts subsumsjonsvalg derfor det mest treffende.

Uansett illustrerer begge dommene at vilkåret om å volde «fare for tap» gjør at for visse saksforhold er det mulig å anvende begge bedrageribestemmelsene. Subsumsjonen beror da på hvor i hendelsesforløpet en anser den kriminelle handlingen som fullbyrdet.

Som nevnt gir derimot forarbeidet uttrykk for at den alminnelige bedrageribestemmelsen skal være den prinsipale påstanden dersom gjerningspersonen «forleder noen».[58] Hendelsesforløp som har element av menneskelig interaksjon eller sosialt element som kan knyttes til

[54] Tilsvarende var tapsvilkåret ved straffeloven av 1902 § 270 første ledd nr. 2.
[55] Ot.prp. nr. 35 (1986-1987) s. 25
[56] Rt. 1995 s. 1704 s. 1706 og Rt. 1996 s. 1673 s. 1674.
[57] Rt. 1995 s. 1704 s. 1706
[58] Ibid.

tapsvilkåret og som ellers oppfyller vilkårene i strl. § 371 bokstav a vil dermed falle inn under den alminnelige bedrageribestemmelsen.

En slik konklusjon bør imidlertid forutsette at en klart kan vise at forledelses-vilkåret i bokstav a er oppfylt, og av hensyn til klarhetsprinsippet bør en vike fra å legge til grunn antakelser tilsvarende Høyesteretts grep i *Teletorg-dommen 1*.

5 Nettbanktapping: Bedrageri eller databedrageri?

5.1 Rt. 2012 s. 1968

I Rt. 2012 s. 1968, *Nettbanktapping-dommen*, ble databedrageribestemmelsen anvendt. Det tilsier at dommen er egnet til å eksemplifisere en handling som faller inn under databedrageribestemmelsen. Juridisk teori stiller imidlertid spørsmål ved subsumsjonsvalget i saken. Professor Sunde ved Politihøyskolen påpeker at den kriminelle fremgangsmåten i realiteten var «basert på forledelse av nettbankkunden».[59] Kjernen ved databedrageribestemmelsen er derimot at bedrageriet blir begått overfor en databehandling fri for menneskelig medvirkning. Sunde mener forledelsen av nettbankkunden taler for at handlingen heller skulle vært bedømt som alminnelige bedrageri.[60] Spørsmålet er om rettens vurdering viser hvorfor saken falt inn under databedrageribestemmelsen, om det var rett subsumsjon, og subsumsjonens eventuelle betydning for den overordnede problemstillingen.

Tiltalte hadde medvirket til såkalt «automatisk nettbanksvindel», som innebar å uberettiget skaffe seg tilgang til en annens bankkonto for å så sørge for transaksjoner til egen konto – uten at kontoinnehaver er kjent med transaksjonene som tapper bankkontoen. Tingretten domfelte vedkommende for medvirkning til overtredelse av databedrageribestemmelsen. Anken for Høyesterett gjaldt kun straffutmålingen, og lovanvendelsen ble ikke behandlet. Tilsvarende var situasjonen ved lagmannsrettens ankebehandling, med unntak av at det for et av hendelsesforløpene ble vurdert om nedre grense for straffbart forsøk var passert. Lagmannsrettens avgjørelse inneholder imidlertid en redegjørelse av fremgangsmåten benyttet for nettbanktappingen, og gir dermed grunnlaget nødvendig for å vurdere Sundes problematisering av rettens subsumsjon.[61]

5.2 Rett(ens) subsumsjon?

[59] Sunde (2016) s. 133
[60] Ibid.
[61] Se LE-2011-206856 for lagmannsrettens behandling.

Nettbanktappingen ble utført ved at nettbankkunder, uten å mene det, lastet ned programvare som infiserte datamaskinene deres med en «trojaner» som var «automatisk operativ». Trojaneren infiserer maskinen med en angrepskode, som så sørger for at det i kundens nettbank blir lagt inn overføringer og transaksjoner til de kriminelle som ikke er synlig for nettbankkunden. Ved neste innlogging vil nettbankkunden etter å ha tastet inn engangskoden bli bedt om å taste inn en engangskode enda en gang. Annengangs engangskode-inntasting medfører en godkjenning av tidligere innlagte transaksjoner.[62] Det setter i gang gjennomføring av transaksjonene, som er en «automatisert databehandling» jf. straffeloven § 371 bokstav b.

Som Sunde påpeker er det imidlertid nettbankkundens inntasting av engangskoden som igangsetter prosessen.[63] Gjerningspersonen har dermed «forledet noen» til å gjøre noe som volder tap eller fare for tap jf. strl. § 371 bokstav a. Videre fremgår det av Ot.prp. nr. 35 (1986-1987) på side 25 at selv hvis vilkårene i databedrageribestemmelsen er oppfylt, så medfører det at «noen» er blitt «forledet» at en i stedet skal anvende den alminnelige bedrageribestemmelsen. Det er derfor grunnlag for å stille spørsmål ved rettens subsumsjon.

Eventuelt kan en se subsumsjonen i lys av hvorvidt det, slik som ved *Teletorg-dommene,* er mulig å se til et tidligere fullbyrdelsestidspunkt for bedrageri i hendelsesforløpet. I det den intetanende nettbankkunden laster ned «trojaner»-programvaren, som automatisk infiserer datamaskinen og så legger inn betalinger til de kriminelle, vil det være oppstått en «fare for tap» ved at det «endrer data eller datasystem». Spørsmålet er om det på dette tidspunktet i hendelsesforløpet er skjedd en endring av data eller datasystem som «uberettiget påvirket resultatet av en automatisert databehandling».

At gjerningspersonen har handlet uten rett er neppe tvilsomt, og vilkåret «uberettiget» er oppfylt. Videre må det foreligge en «automatisert databehandling». At et godkjent betalingsoppdrag gjennomføres er en automatisert databehandling. Det er imidlertid ikke dette tidspunktet i hendelsesforløpet som vurderes, men heller saksforholdet frem til nettbankkunden blir bedt om annengangs engangskode-inntasting. Høyesterett har fastslått et krav om at den uberettigede handlingen må ha «frembragt et resultat» jf. Rt. 1991 s. 532 på side 534. Den uberettigede endringen av nettbankkundens datasystem har ført til annengangs

[62] Se LE-2011-206856
[63] Sunde (2016) s. 133

forespørsel om engangskode, og dermed frembragt et resultat. Det vil si, nedre grense for overtredelse av bestemmelsen kan anses nådd ved den uberettigede endringen av nettbankkundens datasystem.

«Automatisert databehandling» innebærer at et datasystem produserer et resultat basert på informasjonsbehandling fri for menneskelig medvirkning. Generering av forespørsel om engangskode skjer som følge av nettbankkundens inntasting av informasjon, som så blir behandlet av et system fri for menneskelig medvirkning. DNBs datasystem blir dermed ført bak lyset ved at det blir bedt om ny engangskode. Infisering med programvare som medfører at det blir bedt om annengangs inntasting av engangskode kan dermed anses å «uberettiget påvirke resultatet av en automatisert databehandling».

Forarbeidsuttalelsen ved Ot.prp. nr.35 (1986-1987) s. 25 vil imidlertid føre til samme resultat for dette saksforholdet som ved *Teletorg-dommene*, nemlig at der det foreligger forledelse av en eller flere personer så skal en i hovedsak anvende den alminnelige bedrageribestemmelsen. Som Sunde påpeker, ved saksforholdet foreligger det en forledelse av nettbankkunden. Det tilsier anvendelse av § 371 bokstav a.

Spørsmålet er om resultatet blir annerledes om en ser subsumsjonen i lys av at bedrageriet ble utført som en såkalt «automatisk» nettbanksvindel.[64] Ordlyden «den som» og «forleder noen», jf. strl. § 371 bokstav a, tilsier for det første at det må være et menneske som blir forledet. For det andre innebærer ordlyden at det må være gjerningspersonen som utfører handlingen eller unnlatelsen som fører til forledelsen. Det er programvaren som har infisert nettbankkundens datamaskin som deretter manipulerer datasystemet som skaper forledelsen hos nettbankkunden. Det vil si at en kan se det slik at gjerningspersonens plassering av trojaner-programvare kun skapte et potensiale for forledelse. Selve forledelsen var videre avhengig av at en rekke forutsetninger måtte falle på plass. På grunn av hendelsesforløpet kan en derfor stille spørsmål om hvorvidt en kan anse det slik at det var den infiserte programvaren ved datamaskinen som forledet nettbankkunden, og ikke gjerningspersonens plassering av programvare. Da *kan* tilfellet vurderes til å ikke falle inn under ordlyden i den alminnelige bedrageribestemmelsen, og at det heller er databedrageribestemmelsen som skal komme til anvendelse.

[64] Omtalt slik i lagmannsrettens behandling, LE-2011-206856

En slik forståelse innebærer imidlertid en svært snever forståelse av kravet om årsakssammenheng. I realiteten foreligger det årsakssammenheng mellom gjerningspersonens plassering av programvare og forledelsen av nettbankkunden, og det medfører at hendelsesforløpet faller inn under ordlyden i den alminnelige bedrageribestemmelsen. Videre vil det ved en slik vurdering fremdeles være slik at det er et menneske som blir forledet. Da er en i hovedsak utenfor databedrageribestemmelsen jf. Ot.prp. nr. 35 (1986-1987) s. 25. Hvorfor ble da saksforholdet behandlet etter databedrageribestemmelsen?

En mulig forklaring kan være at tiltalebeslutningen kun anga påstand om databedrageribestemmelsen, og på grunn av lik strafferamme for de to bedrageribestemmelsene så tingretten det ikke nødvendig å på eget initiativ drøfte den alminnelige bedrageribestemmelsen. En annen forklaring, og som eksempler over har vist, er at det å klarlegge de tilfeller som faller inn under databedrageribestemmelsen kan være en krevende øvelse.

Forarbeidsuttalelser til databedrageribestemmelsen og en nærmere undersøkelse av *Nettbanktapping-dommen* med grunnlag i Sundes problematisering tilsier samlet at de bedrageritilfellene som faller utenfor databedrageribestemmelsen i utgangspunktet kan karakteriseres ved at «noen» på et tidspunkt i hendelsesforløpet er blitt «forledet». Et databedrageri kan dermed i utgangspunktet karakteriseres ved at det *kun* er en maskin som føres bak lyset.

Subsumsjonen av saksforholdet i *Nettbanktapping-dommen* under databedrageribestemmelsen skaper derimot noe tvil ved en slik slutning. Spørsmålet er hvilken betydning denne tvilen skal ha. Da er det viktig å være oppmerksom på at Høyesteretts ankebehandling ikke omfattet lavere instansers lovanvendelse, men gjaldt kun straffeutmålingen. Dette var som nevnt også tilfellet ved lagmannsrettens ankebehandling. Subsumsjonen ble kun gjort ved tingrettens dom.[65] Videre faller saksforholdet inn under ordlyden i den alminnelige bedrageribestemmelsen og det er sikker rett at forarbeidsuttalelser skal tillegges betydelig vekt. Samlet tilsier det at slutningen til Sunde, og som jeg tilslutter, består. Saksforhold som i *Nettbanktapping-dommen* skal subsumeres etter den alminnelige bedrageribestemmelsen. Det tilsier at feil straffebud ble anvendt i *Nettbanktapping-dommen*.

[65] Se TNERO-2011-160768

6 Betalingskortbedrageri: Bedrageri eller databedrageri?

6.1 Faktum og konklusjon

Spørsmålet i LB-2009-7290, *Skimming-dommen 1*, var straffutmåling. Den tiltalte ble domfelt for overtredelse av databedrageribestemmelsen for å ha anvendt skimmede/klonede (falske) kredittkort for mer enn to millioner kroner. Lignende saksforhold forelå ved straffutmålingen i Rt. 2009s. 397, *Skimming-dommen 2*. I Rt. 2014 s. 1097, *Teller-dommen*, var straffutmålingen anket til Høyesterett etter at lagmannsretten hadde dømt de tiltalte for bedrageri ved bruk av forfalskede kredittkort.[66] Alle sakene handler om bruk av forfalskede kredittkort, men subsumsjonsvalget i *Teller-dommen* er ulikt *Skimming-dommene*. Spørsmålet er om en sammenligning kan bidra til å klarlegge hva som karakteriserer de handlinger som faller inn under databedrageribestemmelsen.

I *Skimming-dommen 1* hadde de domfelte ved betalinger på X Cafe brukt forfalskede kredittkort, og de opprinnelige kortene tilhørte AmEx-kunder i Storbritannia og Canada. AmEx bankrepresentant i Norge sørget for oppgjør for bruken, og overførte de aktuelle betalingsbeløpene til Cafe Y Gruppen AS' konto. Kortbruken ved bankterminalene utgjorde en «uberettiget påvirkning av en automatisert databehandling» jf. databedrageribestemmelsen.

I *Skimming-dommen 2* var spørsmålet for Høyesterett hvilken straff tiltalte skulle få for overtredelse av databedrageribestemmelsen på grunn av bruk av skimmede (falske) betalingskort. De forfalskede kortene ble brukt i avtale med bankterminalens innehaver, og ofte uten at varer eller tjenester ble gitt i bytte. Oppgjørsrepresentanten mellom bankterminal-innehaver og kredittkortselskapet for de opprinnelige kortene var Teller AS. Bruken av kortene resulterte i utbetaling fra Teller til innehaveren av bankterminalen, og bruken av kortene var en «uberettiget påvirkning av en automatisert databehandling» jf. databedrageribestemmelsen.

I *Teller-dommen* hadde de tiltalte brukt stjålne og kopierte AmEx kort på kortterminaler til selskapet X Maskin. Selskapet Teller AS ble slik forledet til å overføre omtrent 1,5 millioner

[66] LE-2014-22359

kroner til X Maskin, og Teller ble påført et tap eller fare for tap. Innehaver av selskapet X Maskin var en av de tiltalte, og hadde samarbeidet med øvrige tiltalte i å forlede Teller. Innehaverens kontraktinngåelse om oppgjør for bankterminalen med Teller ble ansett som en «rettsstridig forledelse» av Teller jf. den alminnelige bedrageribestemmelsen.

6.2 Hvem eller hva føres bak lyset?

Det er tydelige likheter ved saksforholdene i de tre dommene: Det benyttes forfalskede kredittkort, kortene anvendes på bankterminaler hvor innehaveren av terminalene er involvert i bedrageriet, og en oppgjørsrepresentant for kredittkortselskapet sørger for utbetaling til den uærlige innehaveren av bankterminalen. Det er naturlig å tenke at lik fremgangsmåte skal tilsi lik subsumsjon. Likevel ble saksforholdet i *Teller-dommen* subsumert under den alminnelige bedrageribestemmelsen. En sammenligning av dommene kan bidra til å klarlegge hva som karakteriserer de handlinger som faller inn under databedrageribestemmelsen.

Lagmannsretten i *Teller-dommen* gjenga sakens bakgrunn og hendelsesforløpet.[67] Det fremgår at oppgjørsavtalen med Teller ble inngått i slutten av juni 2011, hvor på den uberettigede kortbruken så foregikk frem til slutten av august. Det resulterte deretter i en uberettiget utbetaling fra Teller AS. Dermed er det en nærhet i tid mellom kontraktinngåelsen og oppstart av kortbruken som medførte uberettiget utbetaling. En tilsvarende tidsnærhet fremgår ikke av faktumbeskrivelsene i *Skimming-dommene*.

Videre fremgår det av *Teller-dommen* at samarbeidsavtalen med Teller ble inngått med uærlige planer. Bankterminalen ble anskaffet og samarbeidsavtalen inngått med forsett om å tilegne seg en uberettiget vinning. Behandlingen av saksforholdet fokuserte på at forholdene ved kontraktinngåelsen medførte at enhver senere kortbruk innebar en «forledelse» av Teller.[68] *Skimming-dommene* har ikke tilsvarende fokus. Det kan være fordi *Skimming-dommene* har saksforhold med lengre hendelsesforløp eller at samarbeidsavtalen ikke ble inngått med uærlig hensikt. På grunn av manglende opplysninger om dette i dommene er dette imidlertid kun spekulasjoner.

[67] LE-2014-22359
[68] Se også Sunde (2016) s. 131, Sunde uttrykket at det bedragerske-«opplegget» innebar forledelse av ansatte i Teller.

Fra sammenligning av dommene kan en utlede, tilsvarende som slutningene ved kapittel 4 og 5: Rettsanvenderens vurdering av hendelsesforløpet kan ha betydning for om det foreligger en «forledelse» av noen. En kan se *Teller-dommen* som at bedrageritidspunktet ble satt til tidspunktet for kontraktinngåelsen, men ved *Skimming-dommene* var det i stedet tidspunktene for kortbruken som utgjorde bedrageritidspunktene. Følgelig ble «noen» ført bak lyset i *Teller-dommen* jf. strl. § 371 bokstav a, mens det ved *Skimming-dommene* var bankterminalene og deres «automatiserte» betalingsprosess som ble ført bak lyset jf. strl. § 371 bokstav b. Dommene illustrerer også at manglende forledelse av en eller flere personer karakteriserer de handlinger som faller inn under databedrageribestemmelsen.

7 Borttakelse fra automat: Tyveri eller databedrageri?

7.1 Generelt

Forut for vedtakelsen av databedrageribestemmelsen i 1987 avsa Høyesterett i 1982 en kjennelse som siden fikk, og fortsatt har, betydning for grensedragningen mellom tyveri og databedrageri. Høyesteretts konklusjon ble inntatt i forarbeidsdrøftelsen til databedrageribestemmelsen,[69] og var av betydning i Rt. 1990 s. 17 og Rt. 1997 s. 1771 ved spørsmål om handlingene var tyveri eller en form for bedrageri. Felles for alle tre sakene var at uberettiget bruk av betalingskort hadde muliggjort uberettiget borttakelse av penger eller varer. Spørsmålet er hvilke konsekvenser rettsavgjørelsene har hatt for forholdet mellom tyveri- og databedrageribestemmelsen, og deres betydning for hva som karakteriserer handlingene som faller inn under de to bestemmelsene.

7.2 1982-kjennelsen

I Rt. 1982 s. 1818 hadde tiltalte foretatt uttak av kontanter i minibankautomat ved bruk av eget bankkort. Problemet var at uttaket medførte overtrekk på tiltaltes konto, og overtrekket var i strid med avtalen han hadde inngått med banken. Uttaket av kontantene var dermed uberettiget.

Det var som nevnt ingen databedrageribestemmelse i 1982, og dermed ikke grunn til å problematisere betydningen av at bruk av betalingskort overfor minibanken innebærer en automatisert databehandling. Høyesterett vurderte tyveribestemmelsens anvendelse, og la avgjørende vekt på at borttakelsen av kontantene var uberettiget og utgjorde en uberettiget vinning. De konkluderte dermed at tyveribestemmelsen kom til anvendelse.

[69] Ot.prp. nr. 35 (1986-1987) s. 26-27 jf. NOU 1985: 31 ss. 8 og 33

7.2.1 Høyesteretts tolkning og subsumsjon

Grunnlaget for anken til Høyesterett var uriktig lovanvendelse etter at den tiltalte var blitt frifunnet av byretten. Spørsmål for Høyesterett var hvorvidt det var grunnlag for å dømme den tiltalte for tyveri.

Høyesterett foretok en kort behandling av vilkårene i tyveribestemmelsen, og uttrykte at den tiltalte hadde «borttatt» penger som «tilhørte» banken og som var i dens besittelse, og at tiltalte var «uberettiget» til pengene. Det ble dermed ikke foretatt en tolkning av vilkårene, men snarere en konstatering av at vilkårene i den konkrete saken var oppfylt. Sammen med dette poengterte Høyesterett at det var irrelevant at banken hadde utstyrt tiltalte med middelet som muliggjorde handlingen. Avslutningsvis gjorde Høyesterett et rettskomparativt grep, og henviser til en avgjørelse av Högsta Domstolen i Sverige.[70] Avgjørelsen hadde ifølge Høyesterett et tilsvarende saksforhold og konklusjonen der ble at den svenske tyveribestemmelsen kom til anvendelse. Høyesterett konkluderte dermed at byrettens lovanvendelse var riktig, og at den frifinnende dommen ikke kunne bestå.

7.2.2 Konsekvensene av Høyesteretts avgjørelse

Det er lett å tenke at bedrageribestemmelsen kom som en reaksjon på saksforholdet og konklusjonen om tyveribestemmelsens anvendelse i *1982-kjennelsen*. I forarbeidene til databedrageribestemmelsen er det imidlertid uttalt at «subsumsjon under tyveriparagrafen fremdeles vil være det naturlige ved manipulasjoner som direkte overfører besittelsen av penger eller andre ting til gjerningsmannen».[71] Det var dermed ikke Høyesteretts avgjørelse som var årsak til tilblivelsen av databedrageribestemmelsen. Ved samme forarbeidsuttalelse fremgår det at selv om *1982-kjennelsens* saksforhold også passer inn under databedrageribestemmelsen, er det tatt et standpunkt om at Høyesteretts konklusjon skal være avgjørende for subsumsjonsvalget.[72]

[70] Høyesterett henviser til omtalen av den svenske rettsavgjørelsen i «Nytt Juridisk Arkiv 1980» s. 224 flg., se dommen s. 1818
[71] NOU 1985: 31 s. 33
[72] Ibid.

I løpet av 1990-tallet kom to lignende saksforhold opp før Høyesterett, Rt. 1990 s. 17 og Rt. 1997 s. 1771. Høyesterett drøftet subsumsjonsvalgene i lys av *1982-kjennelsen*, og Høyesteretts tidligere subsumsjonsbalg forble stående.

7.3 Rt. 1990 s. 17 og Rt. 1997 s. 1771

I Rt. 1990 s. 17, *Bemerkning-dommen*, domfelte byretten den tiltalte for overtredelse av tyveribestemmelsen på grunn av misbruk av eget minibankkort. Uten dekning på kontoen hadde vedkommende benyttet det til varekjøp. Byretten uttrykte at etter *1982-kjennelsen* er det sikker rett at slikt misbruk skal bedømmes som tyveri.

Høyesterett var imidlertid uenig, og bemerket at *1982-kjennelsen* hadde et saksforhold hvor gjerningspersonen hadde overtrukket egen konto ved kontantuttak fra minibank. Til forskjell var det i *Bemerkning-dommen* uklart for Høyesterett hvorvidt gjerningspersonens misbruk av eget bankkort ble utført overfor en automatisk maskin eller ved «villfarelse» av en annen person. Forarbeidsuttalelser om forholdet mellom tyveribestemmelsen, databedrageribestemmelsen og den alminnelig bedrageribestemmelsen ble anvendt i Høyesteretts argumentasjon.[73] Avgjørende for at Høyesterett ikke lot byrettens lovanvendelse bli stående var manglende klarhet i saksforhold og byrettens domsgrunner.[74] Domstolen vek dermed ikke fra *1982-kjennelsen* og forarbeidenes forståelse av forholdet mellom de tre bestemmelsene.

Til forskjell fra *1982-kjennelsen* og *Bemerkning-dommen* hadde den domfelte i Rt. 1997 s. 1771, *Kortkopi-dommen*, ikke misbrukt eget bankkort. Den uberettigede bruken av bankkort ble gjort med kort fravendt kortinnehaveren eller kopier av slike kort. Anken til Høyesterett omfattet i utgangspunktet ikke byrettens lovanvendelse. Førstvoterende var imidlertid uenig i byrettens oppfatning om at misbruk av kopierte bankkort skulle subsumeres under databedrageribestemmelsen. Rett subsumsjon var tyveribestemmelsen ifølge Høyesterett, og Høyesterett valgte derfor å likevel behandle lovanvendelsen. Førstvoterende viste til forutsetningen i NOU 1985: 31 s. 33 om at tyveribestemmelsen skal anvendes der manipulasjon av kortet som brukes eller selve automaten fører til direkte uttak av enten penger eller varer fra automat. Det ble så vist til at dette er forutsetninger som siden er blitt

[73] NOU 1985: 31 side 29 og 33, Ot.prp. nr. 35 (1986-1987) s. 26
[74] Rt. 1990 s. 17 s. 18

tilsluttet av departementet i proposisjonen og i rettspraksis lagt til grunn at er uttrykk for gjeldende rett.[75] Saksforholdet falt derfor ikke inn under databedrageribestemmelsen.

7.4 Konsekvenser og Uno X-dommen

Uberettiget kontantuttak fra egen konto fra automat er tyveri jf. *1982-kjennelsen*, og er i Ot.prp. nr. 35 (1986-1987) s. 26 fastslått som gjeldende rett. Med *Bemerkning-dommen* og *Kortkopi-dommen* ble det videre fastlagt at også direkte uttak av varer og uttak med en annens kort faller inn under tyveribestemmelsen. Dette er siden blitt stadfestet som gjeldende rett jf. Ot.prp. nr.22 (2008-2009) s. 325 og s. 465.

Både forarbeid og rettspraksis tilsier dermed sammenlagt at der en uberettiget bruker et betalingskort, uansett om det er ens eget, et som tilhører en annen eller kopi av et kort som tilhører en annen, til direkte uttak av kontanter eller varer så skal det behandles som tyveri. At det direkte uttaket skjer ved en automatisert databehandling medfører ikke anvendelse av databedrageribestemmelsen.

Dette gjør LA-2018-53821, *Uno X-dommen*, til en kuriositet. Dommen eksemplifiserer ved delkapittel 2.2.3 anvendelse av databedrageribestemmelsens gjerningsalternativ om å «disponere over et kredittkort eller debetkort som tilhører en annen». Gjerningspersonen ble i tingretten domfelt for overtredelse av databedrageribestemmelsen etter å ha brukt et betalingskort tilhørende en annen til å kjøpe og ta ut drivstoff fra selvbetjente pumper ved Uno X-bensinstasjoner. Handlingen faller inn under ordlyden i databedrageribestemmelsen. I tingretten var gjerningspersonen prinsipalt tiltalt for overtredelse av tyveribestemmelsen og subsidiært databedrageribestemmelsen. Tingretten anvendte databedrageribestemmelsen jf. TNETE-2017-095411.

Forarbeidsuttalelsen om anvendelse av tyveribestemmelsen har betydning for saksforholdet i saken, og taler imot tingrettens konklusjon. Dersom en manipulerer en automat (uberettiget bruk av betalingskort på selvbetjent drivstoff-pumpe) slik at man direkte får ut varer kommer tyveribestemmelsen til anvendelse, jf. Ot.prp. nr. 35 (1986-1987) s. 26. Saksforholdet skulle i så tilfelle etter gjeldende rett i stedet vært subsumert under tyveribestemmelsen jf. Ot.prp. nr. 22 (2008-2009) s. 325 jf. Ot.prp. nr. 35 (1986-1987) s. 26.

[75] Ot.prp. nr. 35 (1986-1987) s. 26 og Rt. 1990 s. 17.

En finner videre støtte for en slik forståelse i nevnte *Kortkopi-dommen*. Det fremgår der at rettspraksis har lagt til grunn at forutsetningene i overnevnte forarbeid skal følges,[76] og videre at det ikke er av betydning for subsumsjon etter tyveribestemmelsen at «automaten gir tilgang på varer – for eksempel **bensin** […]» i stedet for penger.[77] Dette tilsier at rett subsumsjon etter både forarbeid og rettspraksis ville vært tyveribestemmelsen.

Om valget av databedrageribestemmelsen peker tingretten i sin vurdering på at den var angitt som subsidiær tiltale og videre at «[e]tter rettens vurdering faller handlingene det her er snakk om mer naturlig inn under bedrageri enn tyveri.» Det blir ikke gitt en ytterligere begrunnelse for subsumsjonsvalget, hverken hvorfor retten valgte databedrageribestemmelsen eller hvorfor de vek tilbake fra å anvende tyveribestemmelsen. En videre drøftelse av tingrettens subsumsjonsvalg vil dermed kun bestå av spekulasjoner, og faller utenfor oppgavens problemstilling.

De sparsomme domsgrunnene gjør ingenting for å styrke tingrettsavgjørelsens utgangspunkt om lav rettskildemessig vekt. Forarbeider og høyesterettspraksis om lignende saksforhold tilsier dermed at tingrettens anvendelse av tyveribestemmelsen kun er en kuriositet og blir en eksemplifisering av utfordringene som kan oppstå i subsumsjonsvalget mellom tyveri og databedrageri.

[76] Bemerkning-dommen (Rt. 1990 s. 17)
[77] Min utheving, se også Kortkopi-dommen s. 1772

8 Karakteristikker og deres anvendelse på moderne lovbrudd

8.1 Hva karakteriser de handlinger som faller inn under …

Avgjørende for å klarlegge grensene mellom handlinger som faller inn under databedrageri- alminnelig bedrageri- og tyveribestemmelsen er det særegne ved bestemmelsenes gjerningsbeskrivelse, tilhørende forarbeidsuttalelser og deres anvendelse i rettspraksis

For databedrageribestemmelsen innebærer det at handlinger som omfattes av straffebudet i hovedsak kan karakteriseres ved at det for det første er krav om at fremgangsmåten for å oppnå den uberettigede vinningen er fri for menneskelig interaksjon. Anvendelse forutsetter at det kun er en datamaskin som blir lurt. Dette fremgår særlig av forarbeidsuttalelsen om at selv der ordlyden i databedrageribestemmelsen er oppfylt, så er det den alminnelige bedrageribestemmelsen som skal anvendes dersom det i hendelsesforløpet foreligger «forledelse» av «noen» jf. Ot.prp. nr. 35 (1986-1987) s. 25.

Følgelig, det at noen på et tidspunkt i hendelsesforløpet er blitt «forledet» av gjerningspersonen utgjør en hovedkarakteristikk for handlinger som faller inn under den alminnelige bedrageribestemmelsen. Dersom rettsanvenderen er i tvil om den begåtte handlingen er et data- eller alminnelig bedrageri må hen derfor foreta en vurdering av hendelsesforløpet. Om det på et tidspunkt har vært en menneskelig interaksjon hvor gjerningspersonen har lurt noen slik at det oppstår (fare for) tap skal hen videre vurdere de resterende vilkårene i den alminnelige bedrageribestemmelsen. Skulle det imidlertid ikke være tilfellet, vil det i stedet være grunnlag for å heller ta stilling til de øvrige vilkårene i databedrageribestemmelsen.

For det andre kan handlinger som faller inn under databedrageribestemmelsen karakteriseres ved at de krenker hensynet til datasikkerhet. En krenkelse av hensynet til datasikkerhet må imidlertid vike om gjerningspersonens handling også innebærer at det er skjedd en foreldelse av noen, og handlingen faller da inn under den alminnelige bedrageribestemmelsen jf. avsnittet ovenfor.

Tilsvarende vern av datasikkerhet foreligger ikke ved handlinger som faller inn under tyveribestemmelsen, som er ment å verne eiendomsretten. Ved subsumsjonstvil mellom databedrageri- og tyveribestemmelsen er det gjeldende rett at krenkelse av eiendomsretten skal gå foran krenkelsen av datasikkerhet.[78] Det innebærer at handlinger som faller inn under tyveribestemmelsen kan karakteriseres ved at gjerningspersonen med tilegnelsesforsett oppnår besittelsen av en ytelse, og at databedrageribestemmelsen motsetningsvis kan karakteriseres ved at slike handlinger ikke faller inn under strl. § 371 bokstav b. Ved spørsmål om det er databedrageri- eller tyveribestemmelsen kommer til anvendelse må en derfor ta stilling til ytelsens art, jf. kravet om at det må skje en besittelsesforrykkelse, og hvorvidt besittelse er oppnådd med et tilegnelsesforsett. Foreligger ikke karakteristikken for handlinger som faller inn under tyveribestemmelsen er det grunnlag for å vurdere databedrageribestemmelsen.

Ved kommende behandling av de moderne lovbruddene beskrevet i kapittel 3 er det nærliggende å tenke at av betydning for subsumsjonspørsmålet mellom databedrageri- og alminnelig bedrageri, eller databedrageri og tyveri, er hvem som er den fornærmende. Da er det imidlertid viktig å være oppmerksom på at for bedrageribestemmelsene er det kun et krav om at bedrageriet volder tap eller fare for tap «for noen», og at for tyveribestemmelsen er det ikke et krav om at besitter og eier er samme person. Avgjørende for en treffende subsumsjon er dermed heller kjennskap til hva som karakteriserer handlingene som faller inn under de ulike bestemmelsene og deres tilhørende lovforarbeid og rettsavgjørelser.

8.2 Uberettiget uttak av kontanter med bankkort som tilhører en annen

Subsumsjonstvilen som oppstår ved den beskrevne, og forutsatte forsettlige, handlingen er om den faller inn under databedrageri- eller tyveribestemmelsen. Ordlyden i strl. § 371 bokstav b tilsier at uberettiget uttak av kontanter fra automat med bankkort som tilhører en annen faller inn under databedrageribestemmelsen.

Derimot, karakteristikkene ved de handlinger som faller inn under tyveribestemmelsen er også til stede ved det beskrevne tilfellet. Kontanter er en ytelse som kan bli utsatt for besittelsesforrykkelse og ettersom det er forutsatt at vedkommende handler med forsett om uberettiget vinning vil en i det aktuelle tilfellet også ha handlet med tilegnelsesforsett.

[78] Grunnlaget for gjeldende rett fremgår av redegjørelsen i kapittel 7.

Krenkelsen av eiendomsretten går foran krenkelsen av datasikkerhet, og tilsier at tyveribestemmelsen kommer til anvendelse.

Samme slutning fremgår av gjennomgangen av tilhørende forarbeid og rettspraksis i kapittel 7. Der gjerningspersonen oppnår et umiddelbart kontant- eller vareuttak som følge av å ha manipulert en automatisert databehandling skal dette straffes som tyveri jf. Ot.prp. nr. 22 (2008-2009) s. 325 og s. 465, Ot.prp. nr. 35 (1986-1987) s. 26, *1982-kjennelsen*, *Bemerknings-dommen* og *Kortkopi-dommen*. Om uttaket blir gjort med eget bankkort eller et bankkort som tilhører en annen er videre irrelevant jf. Rt. 1997 s. 1771 *Kortkopi-dommen*.

I *Norsk spesiell strafferett* på side 324 ved omtalelse av tyveribestemmelsen uttaler Matningsdal at uberettiget borttakelse av bankkortet utgjør tyveri, men at det så foreligger «bedrageri i forhold til banken for de pengene som uttas fra minibanken jf. strl. § 371 bokstav b».[79] Dette er står i motsetning til hva som fremgår av forarbeider og rettspraksis. Når uttalelsen i tillegg ikke er begrunnet med annet enn en henvisning til databedrageribestemmelsen begrenser dette uttalelsens vekt.

Sunde gir, i motsetning til Matningsdal, uttrykk for at rettstilstanden, med grunnlag i nevnte forarbeid og rettspraksis, medfører at det beskrevne tilfellet skal subsumeres etter tyveribestemmelsen.[80] Det avgjørende for subsumsjonen er ifølge Sunde ytelsens karakter – at der gjerningspersonen oppnår en gjenstand, og ikke en tjeneste eller et elektronisk pengebeløp, er det tyveribestemmelsen som kommer til anvendelse.[81]

Tilsvarende forståelse av rettstilstanden og henvisning til rettskilder fremgår hos Andenæs i *Spesiell strafferett og formuesforbrytelsene* (2008), hvor det på side 314 fremgår at dersom en får ut penger eller varer fra en automat ved å bruke et manipulert kort eller manipulerer selve automaten, er dette tyveri. Og videre, at også uberettiget bruk av en annens betalingskort til å «heve penger» må bedømmes som tyveri.[82] Forarbeidene har som nevnt likestilt kontant- og vareuttak fra automat, og Andenæs' kommentar om å «heve penger» sett i lys av hans

[79] Matningsdal (2021) s. 324.
[80] Sunde (2016) s. 125-127.
[81] Sunde (2016) s. 131.
[82] Andenæs' bok behandler straffeloven av 1902, men viser til samme tidligere forarbeider og rettspraksis som fremgår av Ot.prp. nr. 22 (2008-2009) s. 325. Videre fremgår det som nevnt av forarbeidene til dagens bedrageribestemmelser og tyveribestemmelse at straffeloven av 2005 ikke medførte en realitetsendring. Andenæs' uttalelse er dermed relevant.

forutgående uttalelse leses dermed ikke som at det kun er ved uberettiget *kontant*uttak at han mener tyveribestemmelsen kommer til anvendelse, men at også vareuttak omfattes.

Videre har Matningsdal i *Straffeloven. De straffbare handlingene* gitt uttrykk for tilsvarende forståelse av rettstilstanden som Sunde og Andenæs. Ved redegjørelse av strl. § 321 om tyveri omtaler han Rt. 2009 s. 397 *(Skimming-dommen 2*) på side 814, og gir med henvisning til Rt. 1997 s. 1771 (*Kortkopi-dommen*) uttrykk for at tilfellet skulle vært subsumert som tyveri. Matningsdal erkjenner dermed tyverisubsumsjon ved tilfeller som tilsvarer det beskrevne tilfellet. Videre, ved behandlingen av databedrageribestemmelsen utrykker han på side 985-986 at «[m]isbruk av bankkort til direkte uttak eller manipulering av automat, skal derimot fortsatt staffes som tyveri» og henviser til NOU 1985: 31 s. 33, Ot.prp. nr. 35 (1986-1987) s. 26, Ot.prp. nr. 22 (2008-2009) s. 464 og hans egen kommentar til § 321. Matningsdal virker dermed her å gi uttrykk for en annen oppfatning enn i *Spesiell strafferett*, og har for sin forståelse av rettstilstanden en henvisning til andre rettskilder enn kun straffebudet.

I lys av annen juridisk teori og at det ved Matningsdals kommentar om databedrageri-subsumsjon i *Spesiell strafferett* ikke er argumentasjon for en eventuell adgang til å endre rettstilstanden, fremstår kommentaren som en enslig svale. Øvrige gjennomgåtte rettskilder tilsier samlet at et uttak av kontanter eller varer fra automat ved det beskrevne tilfellet skal subsumeres som tyveri.

8.2.1 Bør rettstilstanden endres?

Sunde argumenterer for at rettstilstanden bør endres.[83] Ved Høyesteretts subsumsjon i *1982-kjennelsen* var det ingen databedrageribestemmelsen, og det fremtredende ved gjerningspersonens handling var hans uberettigede borttakelse av en gjenstand (kontanter). Tyveribestemmelsen var derfor passende. Etterfølgende høyesterettspraksis og lovforarbeid har sett hen til *1982-kjennelsen* og tilsvarende vurdert at det er den uberettigede borttakelsen av en gjenstand som skal avgjørende for subsumsjonen. Derimot forutsetter borttakelsen av gjenstanden at gjerningspersonen uberettiget påvirker en automatisert databehandling, jf. strl. § 371 bokstav b, og det tilsier at det fremtredende ved lovbruddet heller er at en datamaskin føres bak lyset. Det fremstår dermed mer nærliggende å vektlegge ordlyden i strl. § 371 bokstav b, noe som kan eksemplifiseres ved tingrettens subsumsjon i *Uno X-saken*. Der

[83] Sunde (2016) s. 127

uttaler retten at databedrageribestemmelsen kom til anvendelse fordi det var rettens vurdering at handlingene det var snakk om «mer naturlig [falt] inn under bedrageri enn tyveri». Dette ble lagt til grunn av tingretten som følge av ordlyden i de to bestemmelsene, og uten nærmere argumentasjon eller behandling av andre rettskilder.

Videre er grunnlaget for rettstilstanden uoversiktlig. På grunn av hva som egentlig er en klar ordlyd i strl. § 371 b forutsetter derfor subsumsjon i tråd med rettstilstanden at en har god kjennskap til alle relevante forarbeider og rettspraksis. Slik Sunde påpeker er dette unødig komplisert.[84] Samlet er det derfor gode grunner til at det beskrevne tilfellet heller skal falle inn under databedrageribestemmelsen.

De gode grunnene er imidlertid ikke alene tilstrekkelig for en endring av rettstilstanden. En kan ikke se bort ifra at det i lovforarbeidene er klare føringer om at det beskrevne tilfellet, på grunn av høyesterettspraksis, skal subsumeres som tyveri. En endring av rettstilstanden er derfor lovgivers ansvar.

8.3 Uberettiget tilegnelse av strøm

Det beskrevne tilfellet av uberettiget tilegnelse av strøm er fri for «forledelse» av «noen», og subsumsjonstvilen står dermed mellom databedrageri- og tyveribestemmelsen. Ettersom rettspraksis og forarbeid gir uttrykk for at tyveribestemmelsen i utgangspunktet skal gå foran databedrageribestemmelsen i de tilfeller der begge gjerningsbeskrivelser er oppfylt begynner jeg med karakteristikkene ved tyveribestemmelsen.

Strømmen blir forbrukt, og det foreligger et tilegnelsesforsett. Den uberettigede vinningen oppstår ved at gjerningspersonen endrer programvaren ved den automatiske strømmåleren slik at den underrapporterer forbruket til strømselskapet, som så, ved automatiske prosesser, sender ut en uriktig faktura. Det foreligger ikke en typisk besittelsesforrykkelse, og det tilsier at tyveribestemmelsen ikke kommer til anvendelse.

På den annen side, ved den tradisjonelle subsumsjonen av uberettiget tilegnelse som tyveri foreligger det heller ikke en typisk besittelsesforrykkelse. Det tilsier at tyveribestemmelsen likevel kan komme til anvendelse.

[84] Ibid.

Til forskjell fra den tradisjonelle subsumsjonen er det imidlertid ikke slik at gjerningspersonen forbruker strømmen utenom strømmåleren, men foretar som nevnt en uberettiget endring av programvaren til strømmåleren. Det fremtredende ved en slik handling er at gjerningspersonen krenker hensyn til datasikkerhet, og ikke en krenkelse av en annens eiendomsrett. Det tilsier at tilfellet i stedet oppfyller karakteristikkene ved de handlinger som faller inn under databedrageribestemmelsen, og at det derfor er databedrageribestemmelsen som kommer til anvendelse.

I tillegg faller tilfellet mer naturlig inn under ordlyden i databedrageribestemmelsen enn tyveribestemmelsen, og hensyn til forutberegnelig og forståelig rettsanvendelse tilsier at subsumsjonen skal gjøres etter databedrageribestemmelsen.

8.4 Gjentakende tilegnelse av gratis prøveperiode til digitalt abonnement

Ved det beskrevne tilfellet av gjentakende tilegnelse av gratis prøveperiode til digitalt abonnement foreligger det ingen menneskelig interaksjon, og det er derfor ingen som blir «forledet». Anvendelse av den alminnelige bedrageribestemmelsen er utelukket. Videre foreligger det heller ingen ytelses som oppfyller kravene ved tyveribestemmelsen, ei heller en besittelsesforrykkelse. Anvendelse av tyveribestemmelsen er dermed også utelukket. Igjen står databedrageribestemmelsen.

Det foreligger en «uberettiget påvirkning av en automatisert databehandling» fordi gjerningspersonen overfor programvaren anvender «uriktige opplysninger» i registreringen for gratis prøveperiode jf. strl. § 371 bokstav b. Gjerningspersoner benytter uriktige opplysninger overfor en automatisert databehandling for å oppnå den uberettigede vinningen, og krenker dermed hensyn til datasikkerhet. Oppfyllelsen av karakteristikker ved databedrageribestemmelsen tilsier at § 371 bokstav b kommer til anvendelse. Neste spørsmål er om vilkårene «uberettiget vinning» og «volder tap eller fare for tap» i strl. § 371 bokstav b er oppfylt.

Ettersom én gratis prøveperiode er tilgjengelig for alle vil vilkåret «uberettiget vinning» ikke være oppfylt ved førstegangs-registrering. Ved annengangs-registrering har imidlertid gjerningspersonen brukt opp sin gratis prøveperiode, og tilgangen til tjenesten utgjør en «uberettiget vinning».

Videre, ettersom avtalen innebærer at man etter endt gratis prøveperiode skal begynne å betale for tjenesten om en ønsker fortsatt tilgang, vil manglende betaling samtidig som man i realiteten benytter seg av tjenesten, innebære en tapt inntekt for tilbyderen. Handlingen kan også sees i lys av åndsverksloven § 99 som gir uttrykk for forbud mot å omgå tekniske beskyttelsesmurer.[85] Registrering med falske opplysninger for å få tilgang til den eksemplifiserte strømmetjenestene kan en trolig anse som omgåelse av beskyttelsesmuren for å få tilgang til eksemplarene hos tjenesten. Annengangsregistrering med falske opplysninger overfor den automatiserte databehandlingen vil dermed volde tilbyderen «tap». Alle vilkårene i strl. § 371 bokstav b er oppfylt, og databedrageribestemmelsen er aktuell for tilfellet.

Dersom en forandrer litt på faktumet, og forutsetter at tilbudet om gratis prøveperiode ikke er tilgjengelig for «alle og enhver», men for eksempel er forbeholdt en avgrenset krets kan resultatet bli annerledes ved førstegangs-registrering. Tilbudet kan for eksempel være forbeholdt studenter. Om en så uriktig registrerer seg som student oppnår vedkommende en «uberettiget vinning», og tilbyderen leverer en tjeneste de reelt skulle ha mottatt betaling for. Det er dermed voldt «tap», og vilkårene i strl. § 371 bokstav b vil være oppfylt allerede ved førstegangsregistrering.

[85] Lov 15. juni 2018 nr. 40 om opphavsrett til åndsverk mv.

Kilderegister

Norske lover og forskrifter

Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven)

Lov 22. mai 1902 nr. 10 om straff, Almindelig borgerlig Straffelov (Straffeloven)

Lov 20. mai 2005 nr. 28 om straff (straffeloven – strl.)

Lov 15. juni 2018 nr. 40 om opphavsrett til åndsverk mv., (åndsverkloven)

FOR-2011-06-24-726, Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.

Internasjonale konvensjoner

Den europeiske menneskerettighetskonvensjon (EMK)

European Cyber Crime Convention (ETS No. 185 2001)

Norske lovforarbeid

NOU 1985: 31	Datakriminalitet
Ot.prp. nr. 35 (1986-1987)	Om endringer i straffeloven (datakriminalitet)
NOU 2002: 4	Ny straffelov
Ot.prp. nr. 8 (2007-2008)	Om lov om endringer i straffeloven 20. mai 2005 nr. 28 mv. (skjerpende og formildende omstendigheter, folkemord, rikets selvstendighet, terrorhandlinger, ro, orden og sikkerhet, og offentlig myndighet
Ot.prp. nr. 22 (2008-2009)	Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon – sluttføring av spesiell del og tilpasning av annen lovgivning)

Norske rettsavgjørelser

Høyesterett

Rt. 1975 s. 473

Rt. 1982 s. 1816

Rt. 1990 s. 17

Rt. 1990 s. 955

Rt. 1991 s. 532

Rt. 1994 s. 740

Rt. 1995 s. 1704

Rt. 1995 s. 1872

Rt. 1996 s. 1673

Rt. 1997 s. 1771

Rt. 2009 s. 397

Rt. 2009 s. 683

Rt. 2012 s. 622

Rt. 2012 s. 1968

Rt. 2014 s. 1097

HR-2020-955-A

HR-2020-2019-A

HR-2021-2556-A

HR-2022-2468-A

Underinstanser

LB-2009-7290

LG-2009-907-2

LE-2011-206856 (tilhørende tingrettsavgjørelse er TNERO-2011-160768)

LE-2014-22359

LA-2018-53831 (tilhørende tingrettsavgjørelse er TNETE-2017-095411)

Litteratur

Andrej Saving, *EU Internet Law: Second Edition* (Cheltenham, UK, Edward Elga Publishing 2017)

Johs. Andenæs, *Spesiell strafferett og formuesforbrytelsene* (samlet utgave ved Kjell V. Andorsen, Oslo, Universitetsforlaget 2008*)*

Jon Bing mfl., *Innføring i telekommunikasjonsrett* (Oslo, Cappelen Akademiske Forlag 2001)

Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet* (Bergen, Fagbokforlaget 2016)

Inger Marie Sunde, «Har vi behov for straffebud om datakriminalitet?» (2019) i Tidsskrift for strafferett 19(2), 168-185

Inger Marie Sunde, «Datakrimretten i «fugleperspektiv»» (2019) i Tidsskrift for strafferett, 19(2), 129-147

Kripos – den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet, *Cyberkriminalitet 2023: Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer* (Kripos ved Politidirektoratet, 2023), side 6

Magnus Matningsdal *Straffeloven: De straffbare handlingene: Kommentarutgave* (Oslo, Universitetsforlaget 2017)

Magnus Matningsdal *Norsk spesiell strafferett* (Bergen, 3. utgave, Fagbokforlaget 2021)

Nettartikler

Eirik Rossen, «databehandling» (*Store norske leksikon*, 22. september 2021) <https://snl.no/databehandling> besøkt 20. februar 2023

Jannicke Nilsen, «Norske nettselskap er enige: AMS utgjør en risiko for datasikkerheten» (*Teknisk ukeblad*, 1. september 2015) <https://www.tu.no/artikler/norske-nettselskap-er-enige-ams-utgjor-en-risiko-for-datasikkerheten/275560> besøkt 31. januar 2023

Leif Hamnes, «Tappet kraftselskap for 2,3 milliarder» (*E24*, 22. april 2012) <https://e24.no/teknologi/i/G1Ebmq/tappet-kraftselskap-for-23-milliarder> besøkt 31. januar 2023

Nasjonal kommunikasjonsyndighet, «Alle nummerserier for norske telefonnummer» (*Nasjonal kommunikasjonsmyndighet*) <https://www.nkom.no/telefoni-og-telefonnummer/telefonnummer-og-den-norske-nummerplan/alle-nummerserier-for-norske-telefonnumre#8_og_12sifrede_nummer> besøkt 23. mars 2023

NVE, «AMS» (*Norges vassdrag- og energidirektorat*, 27. oktober 2015) <https://www.nve.no/reguleringsmyndigheten/kunde/nett/ams/> besøkt 31. januar 2023

Ragnar Johnsen «teletorg» (*Store norske leksikon*, 28. september 2021) <https://snl.no/teletorg> besøkt 21. februar 2023

Victoria Marie Nordahl; Kjetil Samuelsen, «Kunder svindlet fra bankens eget telefonnummer: - Simpelt gjort» (NRK, 13. mai 2022) <https://www.nrk.no/sorlandet/kunder-svindlet-fra-bankens-eget-telefonnummer-1.15961171> besøkt 24. mars 2023

Wikipedia, «Alfanummer» (*Wikipedia*, sist redigert 30. desember 2015) <https://no.wikipedia.org/wiki/Alfanummer > besøkt 23. mars 2023

Økokrim, «Investeringsbedrageri knyttet til kryptovaluta» (*Økokrim*, 08. mars 2023) <https://www.okokrim.no/investeringsbedrageri-knyttet-til-kryptovaluta.6589188-562360.html> besøkt 21. mars 2023

Lovkommentar

Erling Johannes Husabø ved Lovdata, Karnov lovkommentar note 7 ved straffeloven 2005 § 371 bokstav a

Magnus Matningsdal ved Rettsdata, Norsk lovkommentar note 2322 til straffeloven 2005

Magnus Matningsdal ved Rettsdata, Norsk lovkommentar note 2322 til straffeloven 2005