Datainnbrudd – strl. § 145 annet ledd

En juridisk oppgave

BACHELOROPPGAVE (OPPG300)

Politihøgskolen

2015

Kand.nr: 485

Antall ord: 6543

Innholdsfortegnelse

«Det er en endring fra tilfeldige og opportunistiske angrep til mer avanserte og fokuserte operasjoner mot spesifikke mål av høy økonomisk eller samfunnsmessig verdi.» [1]

1. Innledning

Temaet for bacheloroppgaven min er datainnbrudd. Dette er en sentral del av datakriminaliteten og blir ofte omtalt som datasnok eller hacking. Grunnen til at jeg ønsket å skrive om dette er fordi det er et tema som engasjerer meg personlig og stadig blir mer aktuelt.

Nasjonal sikkerhetsmyndighet anslo i 2011 at kostnadene av datakriminalitet i Norge lyder på 20 milliarder kroner i året. [2] Kostnadene er altså enorme og det er en relativt ny kriminalitetstype som har hatt en eksplosiv utvikling, sammen med informasjonsteknologien, siden 90-tallet.

I dag finnes informasjonsteknologien stort sett overalt. Det være seg i alt fra PCer, TVer og mobiltelefoner til bankkortleseren i butikken, styreenhetene i biler og serversystemet til banken din. Dersom man går tilbake til 80-tallet så var utbredelsen av de nevnte innretningene langt mindre. I tillegg var ikke informasjonsteknologien på langt nær like utviklet som den er i dag.

Det er ingen tvil om at informasjonsteknologien har drøssevis av positive sider. Den kan blant annet forenkle, effektivisere og redusere risikoen i oppgaver for oss. Videre benyttes den på omtrent alle arenaer, både i hjemmene, skolen, idretten, industrien, politiet, forskningen og mange flere.

På den andre siden kan det få negative konsekvenser dersom uvedkommende får muligheten til å påvirke. Hva hvis en person med onde hensikter kunne påvirke datasystemene som styrer et atomkraftverk, alle dørene på en politistasjon eller nettbanken din?

I løpet av praksisåret fattet jeg interesse for hvordan politiet håndterer datakriminaliteten. Min oppfatning er at Kripos[3] har mest kompetanse om datakriminalitet i politiet, og at det generelt i etaten skorter på slik kunnskap.

[1] Nasjonal sikkerhetsmyndighet (2011). Rapport om sikkerhetstilstanden s. 8. Hentet fra: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2011.pdf (april 2015)
[2] Nasjonal sikkerhetsmyndighet (2011). Rapport om sikkerhetstilstanden s. 7. Hentet fra: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2011.pdf (april 2015)

I denne oppgaven skal jeg bl.a. ta for meg en sentral straffebestemmelse innenfor datakriminaliteten og drøfte meg frem til rettsregelen for denne. Bestemmelsen er almindelig borgerlig straffelov (straffeloven eller strl.) 22. mai 1902 nr. 10 § 145 annet og tredje ledd, og omhandler datainnbrudd og et straffeskjerpende ledd til denne bestemmelsen.

2. Avgrensning

I straffeloven finnes det flere bestemmelser som retter seg mot datakriminalitet. Datakriminalitet kan deles inn i tre kategorier:

«- Endring og ødeleggelse (sletting av data;
- urettmessig innsyn i og bruk av data;
- ulovlig bruk av datautstyr.» [4]

Denne oppgaven angår de handlingene i datakriminaliteten som kan kategoriseres under «urettmessig innsyn i og bruk av data». Som nevnt i innledningen er dette regulert i strl. § 145 annet ledd.

Jeg kommer også til å snakke om datainnbruddsbestemmelsen i lov om straff 20. mai 2005 nr. 28 (straffeloven eller strl.)[5] fordi denne innehar noen interessante endringer i forhold til tilsvarende bestemmelse i straffeloven fra 1902. Jeg kommer ikke til å snakke om ratifikasjonen av Europarådets konvensjon fra 8. november 2001 med norsk lovgivning. Konvensjonen omhandler datakriminalitet og har vært styrende for den norske lovgivningen om datakriminalitet. Det er en interessant vinkling til temaet, men av hensyn til oppgavens lengde så vil det ikke bli videre omhandlet.

3. Oppbygning og metode

Jeg vil begynne med en avklaring av noen begreper tilknyttet datakriminalitet. Disse begrepene har ikke nødvendigvis noen rettslig definisjon, men anvendes i oppgaven. Jeg vil også kort belyse begrepene datakriminalitet og datainnbrudd før jeg går videre.

---

[3] Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
[4] Straffelovrådet (gjengitt i Ot.prp. nr.35, 1986-1987, s.7)
[5] Kalles heretter straffeloven fra 2005

Videre skal jeg se på temaet i et forebyggende perspektiv og hvilke utfordringer som finnes her. Det er først for noen tiår siden datakriminalitet juridisk sett begynte å bli aktuelt. Jeg vil gi en kort innføring i hvordan den juridiske utviklingen på området har vært til nå.

I hoveddelen av oppgaven begynner jeg med å ta for meg strl. § 145 annet ledd. Her skal jeg behandle ett vilkår om gangen og drøfte det ved bruk av juridisk metode. Jeg kommer blant annet til å benytte rettskildefaktorer som lovforarbeider, lovteksten, juridisk litteratur, prejudikater og rettsavgjørelser. På denne måten skal jeg finne frem til rettsregelen, som er den regelen man får frem etter en tolkning av rettskildefaktorene.

Strl. § 145 tredje ledd gir en utvidet strafferamme til bestemmelsen dersom noen straffeskjerpende momenter er til stede. Jeg skal på samme måte ta for meg dette leddet av paragrafen.

Videre skal jeg se på forskjellene mellom datainnbrudd i straffeloven fra 1902 og straffeloven fra 2005. Lovteksten i de to bestemmelsene er ganske forskjellige. Jeg skal drøfte om det har skjedd noen realitetsendringer i bestemmelsen fra straffeloven 1902 til straffeloven 2005, og eventuelt hva disse endringene innebærer.

4. Begrepsavklaringer og definisjoner

4.1 Datakriminalitet

Begrepet har ingen selvstendig juridisk definisjon. Straffelovrådet definerte det som «… kriminalitet hvor utnyttelse av datateknologi har vært vesentlig for overtredelsen» i en utredning om datakriminalitet fra 1985. [6] Med denne definisjonen til grunn faller f. eks. skadeverk og tyveri av datamaskiner (selve gjenstanden) utenfor, fordi tyngden legges på utnyttelsen av datateknologi.

4.2 Datainnbrudd

Politiet har følgende definisjon på sine hjemmesider: «Med datainnbrudd menes det å trenge seg inn i datasystemer for å skaffe seg tilgang til beskyttet informasjon.» [7] Denne definisjonen kan gi

[6] NOU 1985: 31 s.6
[7] Hentet fra politiets internettsider: https://www.politi.no/kripos/datakriminalitet/ (april 2015)

et innblikk i hva jeg skal snakke om videre i oppgaven, men har ikke nødvendigvis noen direkte sammenheng med den juridiske rettsregelen eller lovteksten til datainnbruddsbestemmelsen.

4.3 Data

Begrepet er tvetydig. Det kan f. eks. referere til faget data, en datamaskin og har en juridisk definisjon i § 145 annet ledd. Det er denne sistnevnte definisjonen jeg kommer til å legge til grunn. Forenklet fremstilt er det informasjon eller informasjonsbiter. Mer om dette senere i oppgaven.

4.4 Hacker

En hacker er en person som bl.a. verdsetter utfordringer i det å jobbe seg rundt begrensninger på sitt felt. [8] Feltet er ofte dataprogrammering. Et synonym er datasnok.

5. Et forebyggende perspektiv

I lov om politiet 4. august 1995 nr. 53 (politiloven) § 2 nr. 2 står det at en av politiets oppgaver er å: «forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet».

Politiet jobber også forebyggende når det gjelder datakriminalitet, men dette har vist seg å være et vanskelig felt. For det første uttrykker Datakrimutvalget at det foreligger et registreringsproblem og at mørketallene er store. [9] I mørketallsundersøkelsen fra 2012 estimeres det 44 800 hendelser av datakriminalitet hvorav bare 361 av dem har ført til anmeldelser hos politiet. [10] Det vil si at risikoen for å bli oppdaget er relativt liten. Problemet er kjent for Justisdepartementet som i en proposisjon har skrevet: «Felles for de ulike formene for datakriminalitet er at de ofte har stort skadepotensial, samtidig som oppdagelsesrisikoen er lav.» [11]

Det er ikke uvanlig å inneha datautstyr som kan brukes til å begå datakriminalitet med. Dette gjelder omtrent alle bærbare og stasjonære PCer som folk har i dag. Til og med smarttelefonene kan brukes til datakriminalitet. I følge rutineaktivitetsteorien vil alle mennesker begå lovbrudd så

[8] Hentet fra Wikipedias internettsider: http://no.wikipedia.org/wiki/Datasnok (april 2015)
[9] NOU 2007: 2 s.18
[10] Næringslivets Sikkerhetsråd (2012). Mørketallsundersøkelsen s. 15. Hentet fra: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/moerketall_2012.pdf (april 2015)
[11] Ot.prp.nr.40 (2004-2005) s.31

lenge forholdene ligger til rette for det. [12] Ved at man har en motivert gjerningsperson og mangel på voktere (svært få av tilfellene avdekket) så mangler det bare et tilgjengelig objekt for at lovbrudd skal skje, i følge denne teorien.

Tilgjengeligheten til objektet vil blant annet reguleres av programvarebeskyttelsen til det utsatte systemet og datakunnskapen og -erfaringen til gjerningspersonen. I og med at svært få tilfeller av datakriminalitet blir avdekket og straffeforfulgt så er det i stor grad mangel på voktere. Det mangler dermed bare en motivert gjerningsperson. Rutineaktivitetsteorien oppfylles relativt enkelt på denne typen lovbrudd.

Som et forebyggende tiltak mot datakriminalitet ønsker politiet å bli mer tilstedeværende på internett. [13] I løpet av de siste årene har politiet vist større aktivitet på sosiale medier. Det er ikke uvanlig at politiet er aktive på både Facebook[14] og Twitter[14]. På denne måten kan politiet bl.a. vise tilstedeværelse på internett og åpenhet for publikum.

Videre har politiet en egen enhet for datakriminalitet som er underlagt Kripos. Enheten er en av de få «vokterne» for datakriminalitet. Selv om sjansen for å bli oppdaget og anmeldt tilsynelatende er neglisjerbar så kan dette ha en allmennpreventiv effekt.

I høyesterettsdom Rt. 2012 s. 1968, som omhandler databedrageri og datainnbrudd i nettbank, blir det skrevet at internettkriminalitet er et økende samfunnsproblem som truer tilliten til betalingsformene vi benytter oss av (avsnitt 30). Videre blir det i samme avsnitt anført at allmennpreventive hensyn tilsier strenge straffer i slike saker.

Etterforskning av datakriminalitet er avansert og krever kompetanse utover det vanlige. [15] Justisdepartementet har tidligere uttalt i proposisjon: «Flere høringsinstanser er inne på at noe av det viktigste når det gjelder bekjempelse av datakriminalitet er å sette i verk tiltak innen politiet for å styrke etterforskningen av slike saker. Det blir bl a foreslått at det bør gis opplæring og informasjon om datakriminalitet innen politi og påtalemyndighet.» [16]

[12] Elisabeth Myhre Lie, I forkant: Kriminalitetsforebyggende politiarbeid, Oslo 2011 s.259
[13] Økt innsats mot datakriminalitet (2012). Hentet fra: https://www.politi.no/kripos/aktuelt/nyhetsarkiv/2012_01/Nyhet_10916.xml (april 2015)
[14] Begge er globale nettsamfunn
[15] Bente Lovise Storruste, Datakriminalitet, Oslo 2014 s.77
[16] Ot.prp.nr.35 (1986-1987) s.19

Som jeg nevnte i innledningen fikk jeg i praksisåret inntrykk av at kunnskapene om datakriminalitet generelt er noe manglende i politietaten. Ved å styrke politiets kunnskaper om etterforskningen og selve datakriminaliteten kunne flere slike lovbrudd blitt oppdaget og endt med reaksjoner fra rettsapparatet. Det er ikke usannsynlig at dette også kunne ført til en noe økt allmennpreventiv effekt. Jeg ønsker at denne oppgaven kan være et bidrag til klargjøringen av datakriminalitet, herunder datainnbrudd.

6. Datakriminalitet og rett i historisk perspektiv

Informasjonsteknologien har, som jeg nevnte, hatt en enorm utvikling siden 80-tallet. I kjølvannet av utviklingen følger også kriminalitet ved utnyttelse av datautstyret. Datakriminalitet fantes også før dette, men da i mye mindre grad.

Det som da ble kalt «justis og politidepartementet» avla i 1978 en proposisjon[17] som inneholdt forslag til endringer i straffeloven 1902. Blant annet ble det foreslått endringer i strl. § 145

«… med sikte på å ramme bl a uberettiget innkobling på telexnettet for å fange opp meldinger til andre, og det at man uberettiget gjør seg kjent med innholdet av lydbåndopptak eller opplysninger lagret ved hjelp av EDB.» [18]

Tidligere hadde denne bestemmelsen bare rammet uberettiget brudd av «brev eller annet lukket skrift». Dette er altså på mange måter fødselen til datainnbruddsbestemmelsen.

I 1983 ga Justisdepartementet Straffelovrådet i oppgave «… å foreta en kartlegging av forskjellige former for datakriminalitet, og å vurdere om det er behov for å endre gjeldende straffebestemmelser med sikte på å ramme straffverdige handlinger på dette området.» [19]

Straffelovrådet besvarte mandatet i 1985 med en utredning[20] om datakriminalitet som inneholdt omfattende endringer i forhold til datidens bestemmelser om datakriminalitet. Det ble bl.a. gjort store endringer i lovteksten til datainnbrudd og den fikk et eget ledd i paragrafen. Før dette var

[17] Ot.prp.nr.4 (1978-1979)
[18] Ot.prp.nr.4 (1978-1979) Se kapittelet «proposisjonens hovedinnhold»
[19] NOU 1985: 31 s.3
[20] NOU 1985: 31

den flettet inn i samme ledd som brevbruddbestemmelsen. Alle de nevnte endringene var med på å danne grunnlaget for hvordan bestemmelsen om datainnbrudd ser ut i dag.

7. Straffeloven § 145 annet ledd

Lovteksten lyder:

«Det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler.»

Lovteksten viser til strafferammen som er beskrevet i straffebudets første ledd ved at det står «Det samme gjelder…». Strafferammen er bøter eller fengsel inntil 6 måneder eller begge deler. Den ble hevet til dette etter forslag fra justis- og beredskapsdepartementet i 2004. [21] Hensikten med den utvidede strafferammen var å åpne for bruk av straffeprosessuelle tvangsmidler. [21]

7.1 Bestemmelsens formål

Bestemmelsens formål er å beskytte integritetshensynet og den allmenne interessen for konfidensialitet. [22] Dette kommer uttrykkelig frem i lovforarbeider[22] og Høyesterett har uttalt det i Rt. 2004 s. 94 (avsnitt 18). Den beskytter også vederlagsinteressen. [22]

Videre står det i lovforarbeidene at det med integritetshensynet menes nødvendigheten av å kunne sette sin lit til datasystemers pålitelighet. [22] Det er ønskelig at man skal kunne ha tillit til datasystemene som informasjonen er lagret i. Integritetshensynet kan krenkes på flere måter. Et praktisk eksempel er når hackeren har oppnådd uberettiget tilgang til kundedataene til en bedrift. Integriteten krenkes da ved at den utsatte da mister kontrollen over dataene eller brukerne sine.

Vernet av konfidensialiteten kan sies å være et vern for den private omgang med elektronisk informasjon og tjenester. [23] Vernet fremmer rettsgodet om privatlivets fred som Norge har forpliktelser om gjennom lov om styrking av menneskerettighetenes stilling i norsk rett 21. mai 1999 nr. 30 (menneskerettsloven) § 2, jf. EMK[24] art. 8. Et ord som ofte brukes synonymt med «konfidensialitet» er «hemmelig». I datainnbruddsbestemmelsen skal ikke konfidensialitet forstås

[21] Ot.prp.nr.40 (2004-2005) s.33
[22] NOU 2003:27 s.14
[23] Inger Marie Sunde, Lov og rett i cyberspace, Oslo 2006 s.117
[24] Den europeiske menneskerettighetskonvensjonen

på denne måten. Det er ikke noe krav eller vilkår at dataene eller informasjon må være hemmelig. Jeg skal se nærmere på dette i drøftelsen nedenfor.

Vederlagsinteressen handler om den kommersielle verdien av dataene. [25] Dette kan f. eks. dreie seg om bedrifter som har egne hjemmesider tilknyttet servere med kundeinformasjon. Et praktisk eksempel på en slik bedrift er Telenor.

7.2 Skaffet seg adgang

Et av vilkårene i lovteksten er at gjerningspersonen har «skaffet seg adgang».

I lovforarbeidene til bestemmelsen brukes også ordene «innsyn» og «tilgang». Videre står det at overtredelsen kan være fullbyrdet selv om gjerningspersonen ikke har gjort seg kjent med dataene eller programutrustningen. Vilkåret er oppfylt så fort gjerningspersonen har skaffet seg adgang til dem. [26] Det vil si at det har blitt skaffet tilgang, og ikke nødvendigvis at data har blitt eksponert for gjerningspersonen.

Det er integritetshensynet som krenkes når adgangen er skaffet. Dette er fordi den utsatte da mister kontrollen over dataene eller brukerne sine. Dette rokker ved den nødvendige tilliten man må kunne ha til datasystemene i samfunnet. Integritetshensynet beskytter med andre ord dataene indirekte ved at det verner mot den som uberettiget skaffer seg *adgang* til dem og ikke selve befatningen dataene. Den påfølgende konsekvensen av at adgang oppnås er naturligvis som oftest at gjerningspersonen gjør seg kjent med, kopierer, endrer dem e.l.

7.3 Data eller programutrustning

Objektet som det skaffes uberettiget adgang til må være «data eller programutrustning» for at det skal falle innunder normen. Konfidensialitetshensynet, integritetshensynet og vederlagsinteressen ivaretas best ved at det ikke tas hensyn til hvilke data det har blitt skaffet adgang til. Slik er det også i denne bestemmelsen når det gjelder spørsmålet om vilkåret er oppfylt.

I lovforarbeidene står det at begrepet «data» må tolkes vidt. [27] Begrepet omfatter all informasjon og stiller ingen krav til at den må være hemmelig eller lignende. [27] Hvilke data det har blitt

[25] NOU 2003:27 s.14
[26] Inger Marie Sunde s.122
[27] Ot.prp.nr.35 (1986-1987) s.20

skaffet adgang til og hvilken verdi disse har, vil eventuelt bare få betydning i straffeutmålingen. Det spiller således ingen rolle for straffbarheten om man har skaffet seg adgang til ett bilde som er lagret på en harddisk eller adgang til en hel database.

Det finnes på den andre siden grenser for hvor vidt databegrepet kan tolkes. Høyesterettsdommen i Rt. 1994 s. 1610 handler om en person som produserte og omsatte dekodere som kunne brukes for å få inn fjernsynsprogrammer uten samtykke fra rettighetshaveren og som det normalt skal betales for. Her ble det et spørsmål om hvorvidt fjernsynsprogrammene kunne omfattes av databegrepet i strl. § 145 annet ledd. Under dissens (3-2) kom Høyesterett til at det språklig sett ikke var naturlig å forstå begrepet på denne måten og at forarbeidene ikke ga grunnlag for en slik utvidende tolkning (s.1612).

Smartkort-dommen, Rt. 1995 s. 35, handler om en person som hadde «pirat-smartkort» som gjorde det mulig å få inn TV-sendinger uten samtykke fra rettighetshaveren og som det også normalt skulle betales for. I smartkort-dommen vises det til høyesterettsdommen jeg nevnte ovenfor når det gjelder spørsmålet om TV-sendinger kan regnes som data ut i fra strl. § 145 annet ledd (s.36). Resultatet ble dermed ikke overraskende det samme, når det gjelder tolkningen av databegrepet. Senere på året i 1995 ble strl. § 262 opprettet i straffelovens 24. kapittel (underslag, tjueri og ulovlig bruk). Bestemmelsen omhandler nettopp «uberettiget tilgang til vernet formidlingstjeneste».

Programutrustning er det samme som dataprogram. I lovforarbeidene blir det definert som «… instruksjonene til en datamaskin, altså dataprogrammer». [28] Som et vilkår i bestemmelsen er begrepet noe redundant da programutrustning nødvendigvis må være oppbygget av data. Det kan imidlertid bidra til en eksemplifisering og tydeliggjøring av bestemmelsens praktiske virkeområde.

7.4 «Lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler»

Videre må datainnbruddet gjelde data «som er lagret eller som overføres». Dette byr i praksis ikke på problemer fordi data vanskelig kan tenkes å eksistere uten enten å være lagret eller under

[28] Ot.prp.nr.40 (2004-2005) s.12

overføring. Det spiller heller ingen rolle for straffbarheten hvilket av disse vilkårene som er oppfylt.

Data kan være lagret fysisk eller virtuelt; fysisk på DVD-plater, SIM-kort, harddisker eller virtuelt i en nettsky[29]. Data som overføres kan f. eks. være internettrafikk, mobildata og email som sendes. Noe forenklet kan man si at data som er lagret er *informasjon* og data som overføres er *kommunikasjon.*

Videre er det et krav om at dataene som er lagret eller som overføres må være det *ved* «elektroniske eller andre tekniske hjelpemidler». I informasjonsteknologien konverteres signaler ofte mellom å være digitale og analoge. F. eks. er data som er lagret på en harddisk analoge, og må konverteres til digitale før datamaskinen klarer å lese informasjonen. Ved mobiltelefonsamtaler foregår det som regel også en konvertering mellom det digitale og analoge.

I lovforarbeidene står det at: «Henvisningen til at dataene må være lagret, henspeiler på alle former for elektroniske lagringsmedier, herunder harddisk, disketter, CD-ROM, DAT-taper mv.» [30] Det skilles altså ikke mellom digitale og analoge signaler fordi det står «alle former for elektroniske lagringsmedier». I denne datasammenhengen ville en alternativ fortolkning vært kuriøs og kunne skapt vanskeligheter ved lovanvendelsen.

Data kan også være lagret eller overføres ved «andre tekniske hjelpemidler». Vilkåret vil for eksempel kunne omfatte data som overføres via fiberteknologien som benytter seg av dataoverføring via lyssignaler (ikke elektroniske). [31] Det er ikke uvanlig at husstander er koblet til internett ved hjelp av denne teknologien.

7.5 Uberettiget

Videre er det et vilkår at adgangen til dataene er *uberettiget.* Dette vilkåret er på sett og vis nøkkelordet i bestemmelsen og er betydelig omhandlet i både rettspraksis og lovforarbeidene. Bestemmelsen har gjennomgått flere realitetsendringer siden den oppstod i 1979, men rettstridsreservasjonen har stått urørt. Det er ikke uvanlig i rettsaker at uenigheter om datainnbruddbestemmelsens anvendelsesområde skyldes nettopp dette vilkåret.

[29] Serverparker som er koblet til internett
[30] NOU 2003: 27 s.14
[31] Inger Marie Sunde s.123

For at adgangen skal være uberettiget må det være noe med den som kan anses som klander- og straffverdig. [32] F. eks. vil det være uberettiget dersom en person utnytter en svakhet i programutrustningen til en bedrift slik at han får adgang til bedriftens databaser. Dette kalles et sårbarhetsinnbrudd. Derimot kan det neppe anses som klander- og straffverdig dersom en person på alternative måter skaffer seg adgang til dataene i mobiltelefonen sin som han hadde glemt låsekoden til.

Justisdepartementet har uttalt i lovforarbeidene at: «Det beror i prinsippet på lovgivning og avtaler hvilke data en person har rett til å gjøre seg kjent med, men her kan det oppstå vanskelige grensetilfelle.» [33]

Bestemmelsene om datakriminalitet er spesielt aktuelle for arbeidstakere som skal betjene datautstyr. I lovforarbeidene til strl. § 145 annet ledd står det at som en del av vurderingen om innsynet er uberettiget må man trekke inn tariffavtale, arbeidsavtale, stillingsinstrukser og arbeidsrettslige regler. [34] Disse vil ofte være med på å sette grenser for når innsyn og utnyttelse av data er rettsstridig og uberettiget. Det samme gjelder bruken av datautstyret. Dette betyr at spørsmålet om uberettiget adgang i forbindelse med arbeidstakere ofte i praksis vil la seg løse ved å se på hvilke avtaler, regler og instrukser som regulerer arbeidsforholdet.

Mange tilfeller vil være åpenbart uberettigede. La oss si at en gjerningsperson installerer et program på datamaskinen til en bekjent for ham, uten at den bekjente har kjennskap til det. Dette programmet fanger opp innloggingsinformasjonen til nettbanken hans og sender det til gjerningspersonens e-postadresse. Dersom da gjerningspersonen bruker denne innloggingsinformasjonen til å få adgang til hans bekjentes nettbank, så vil denne adgangen åpenbart være uberettiget. Det forelå da ikke noen form for samtykke eller avtale fra vennen til å gjøre dette.

Et litt mer komplekst tilfelle, som kan ligne på dette, er Photobucket-dommen, Rt. 2012 s. 1669. Her hadde fornærmede fått virus på PCen sin og var bekjent med tiltalte som visstnok skulle være flink med datamaskiner. Det ble avtalt at tiltalte skulle forsøke å reparere PC-en til fornærmede og han fikk i denne anledning innloggingspassordet til den.

[32] Inger Marie Sunde s.145
[33] Ot.prp.nr.35 (1986-1987) s.9
[34] Ot.prp.nr.35 (1986-1987) s.21

På fornærmedes PC lå det bl.a. kontonummer, kredittkortnummer, private bilder og passord til e-postkontoer. Dette kopierte tiltalte over til sin egen datamaskin. Aktor understrekte at man ved lovtolkningen måtte vektlegge vilkåret «uberettiget». Gjerningspersonen skulle fikse PCen og hadde ikke rett til å gå inn på lagrede data.

Tiltalte anførte at han ble gitt tilgang ved at han lånte PCen og fikk innloggingsdetaljene. Høyesterett kom frem til at adgangen ikke var uberettiget (avsnitt 26). Ved at tiltalte fikk PCen, innloggingsdetaljer og tillatelse til å undersøke fornærmedes PC *i sin helhet*, var ikke adgangen til dataene som ble tilgjengelige for ham etter innloggingen, uberettiget.

7.6 Skyldkrav

Skyldkravet for datainnbrudd etter strl. § 145 annet ledd er forsett jf. strl. § 40 første ledd. Det følger av det ulovfestede dekningsprinsippet at forsettet må dekke alle vilkårene i gjerningsbeskrivelsen.

For politiets etterforskning av datainnbrudd vil det være sentralt å belyse hvorvidt gjerningspersonen visste om adgangen var uberettiget eller ikke. Altså om rettstridsreservasjonen ble overtrådt med forsett eller ikke.

I tilfellene hvor personen bruker avanserte metoder, f. eks. bruteforce-programmer[35], for å skaffe seg adgang vil det være større sjanse for at adgangen var uberettiget og desto lettere å belyse skyld. I de tilfellene der det ikke har blitt brukt avanserte metoder vil det kunne være vanskeligere. Et eksempel på dette er Photobucket-dommen, Rt. 2012 s. 1669, som jeg var innom under drøftelsen om rettstridsreservasjonen på forrige side.

Skyldspørsmålet i forhold til de øvrige vilkårene vil ofte være enklere å belyse. Å skaffe seg adgang til lagrede data eller data som overføres vil ofte være en aktiv handling. Også språklig sett innebærer det å «skaffe seg» en form for aktiv tilnærming. Dersom noen har skaffet seg adgang til data vil det ofte vanskelig kunne påberopes at dette ikke var med viten og vilje.

Når politiet etterforsker i forbindelse med informasjonsteknologi vil det ofte være viktig å vite *hvem* som var brukeren av utstyret. Metodene for dette er stort sett like for etterforskning av

[35] Programmer som systematisk gjetter innloggingsdetaljer helt til det finner de rette

datainnbrudd som for etterforskning av øvrig kriminalitet i forbindelse med informasjonsteknologi. I denne oppgaven skal jeg ikke gå videre inn på slike metoder.

8. Straffeloven § 145 tredje ledd

Lovteksten lyder:

«Voldes skade ved erverv eller bruk av slik uberettiget kunnskap, eller er forbrytelsen forøvet i hensikt å skaffe noen en uberettiget vinning, kan fengsel inntil 2 år anvendes.»

Dette leddet omhandler straffeskjerpende omstendigheter som skal leses i sammenheng med første eller annet ledd. Tredje ledd er altså ikke noen selvstendig straffehjemmel i seg selv, men en utvidet strafferamme dersom visse vilkår er oppfylt. For at tredje ledd skal kunne anvendes må minst ett av de to straffeskjerpende alternativene være oppfylt, vinningsalternativet eller skadealternativet.

8.1 Skadealternativet

Alternativet nevner «slik uberettiget kunnskap». Dette henviser til «brev eller annet lukket skrift» i første ledd eller «data eller programutrustning» i annet ledd. Et spørsmål som kan dukke opp i forbindelse med dette er om det er *dataene* eller *innholdet* av disse som det er ment at dette straffeskjerpende alternativet skal beskytte.

Språklig sett vil det være normalt å tenke at kunnskapen er innholdet i dataene. Hvis man legger til grunn en slik tolkning av vilkåret ville tilfellene der hvor gjerningspersonen ikke forstod dataene riktig, men voldte skade ved å erverve eller bruke dem, ikke blitt omfattet.

En slik innskrenkende tolkning ville også kunne skapt problemer i forhold til krypterte data. Dette er data som er gjort uleselig for alle andre enn de som har et passord for å åpne krypteringen igjen. Selv om det er svært vanskelig så er det ikke umulig å komme seg forbi krypteringer.

Begrepet «kunnskap» skal ikke tolkes innskrenkende, men det skal brukes en «både-og»-fortolkning. [36] Det betyr at «kunnskap» kan tolkes både som de elektroniske data og som

[36] Inger Marie Sunde s.157

innholdet i informasjonen. Denne uklarheten i bestemmelsen skyldes at det mangler noen redegjørelse på om bestemmelsen er ment å verne data eller innholdet i data. [36]

Videre er «erverv eller bruk» et vilkår i skadealternativet. Vilkårene er ikke kumulative. Det er altså tilstrekkelig at ett av alternativene er oppfylt. En gjerningsperson kan bruke kunnskapen for sine egne- eller andres formål. Gjerningspersonen bruker kunnskapene f. eks. dersom han har kopiert hemmelige produksjonsdetaljer og begynner å produsere selv etter disse.

Det omfattes også som bruk dersom prosessen gjøres via tredjemann. [37] Dvs. at det også ville vært bruk om personen hadde solgt produksjonsdetaljene til en annen som hadde startet produksjon. Vilkåret oppfylles da av begge to. [37]

Erverv kan bare skje på to vis. Enten ved at dataene kopieres eller ved at de leses.

Kravet til skade er annerledes enn hva som gjelder i skadeverkbestemmelsen, jf. strl. § 291. Både økonomisk og ikke-økonomisk skade omfattes. [38] Som nevnt tidligere i oppgaven skal bestemmelsen beskytte bl.a. integritetshensynet og konfidensialitetshensynet. F. eks. kan integritetshensynet krenkes ved at noen gjør innbrudd i en annens datamaskin og bruker denne til å utføre oppgaver. Eieren av den hackede datamaskinen fremstår da som utføreren av oppgavene og hans omdømme kan lide tap. Omdømmetap er et eksempel på skade jf. strl. § 145 tredje ledd. [38] Skade ved krenkelse av konfidensialitet kan f. eks. oppstå ved frigjøring av opplysninger som er taushetsbelagte ved lov.

Det må videre være årsakssammenheng mellom skaden, og ervervet eller bruken av kunnskapen. Dette fremkommer av lovtekstens ordlyd der hvor det står «voldes skade *ved*» (min uth.). Skyldkravet til skaden følger av strl. § 43, 1. ledd. Det er altså tilstrekkelig skyld dersom gjerningspersonen kunne ha innsett muligheten for skaden.

En person ble i lagsmannsretten, RG. 2010 s. 618 (Frostating), domfelt for overtredelse av skadealternativet i strl. § 145 tredje ledd jf. annet ledd. Ved å utnytte en svakhet i Tele2s datasystemer fikk han ut personopplysninger og kredittverdighetsopplysninger om minst 1208 personer uten at han var berettiget til dette. Videre delte han disse opplysningene og

[37] Inger Marie Sunde s.158
[38] Inger Marie Sunde s.159

fremgangsmåten til å skaffe dem på et nettsamfunn med over 40.000 brukere. Tele2 anslo sitt økonomiske tap til 70.000 kr.

Aktor anførte bl.a. at Tele2 sitt renommé hadde blitt svekket samt at opplysningene som ble utsatt for lekkasje var særlig egnet til å skade personene de gjaldt. [39] I dommen vektla lagmannsretten således at Tele2 også hadde blitt påført ikke-økonomisk skade. [40]

8.2 Vinningsalternativet

Dette alternativet er oppfylt dersom forbrytelsen er «forøvet i hensikt å skaffe noen en uberettiget vinning».

«Forbrytelsen» refererer til overtredelsen av strl. § 145 første eller annet ledd. Det som er interessant å se på i dette alternativet er den uberettigede vinnings hensikt. Høyesterett har uttalt i Photobucket-dommen, Rt. 2012 s. 1669, at: «… når en person uberettiget skaffer seg goder med økonomisk verdi til eget bruk, har han vinnings hensikt uavhengig av hva slags personlig motiv han eller hun har» (avsnitt 35). Denne dommen anses som et sentralt prejudikat innenfor retten om datainnbrudd. Saken omhandlet en person som hadde gjort datainnbrudd i bildeopplastningsnettsiden Photobucket Inc sine dataservere og hentet ut opplysninger om over 66 millioner kunder. Høyesterett uttalte videre at kunderegistre må anses å ha økonomisk verdi (avsnitt 36).

Et annet praktisk eksempel på et gode med økonomisk verdi er kredittkortsdata. Godet trenger ikke å være data fra innbruddet. Dersom en hacker har blitt lovet vederlag for et oppdrag som innebærer datainnbrudd, så vil hackeren kunne straffes for uberettiget vinnings hensikt selv om dataene ikke hadde noen økonomisk verdi. [41]

Det fremkommer av lovtekstens ordlyd at forbrytelsen må være *forøvet* med uberettiget vinnings hensikt. Det vil si at denne hensikten tidsmessig må foreligge ved datainnbruddet. Det vil altså falle utenfor dersom en hacker er på vilkårlig utkikk etter et datasystem å skaffe seg adgang til, og når han først har oppnådd denne uberettigede adgangen, så finner han kundeopplysninger som han der og da bestemmer seg for å selge videre.

[39] Dommen mangler sidetall og avsnitt. Se aktors anføringer.
[40] Lagmannsrettens bemerkninger
[41] Inger Marie Sunde s.165

9. Sammenligning mellom ny og gammel straffelov

I straffeloven fra 2005 er det gjort en del endringer i bestemmelsene om datakriminalitet. En sentral endring er opprettelsen av kapittelet som heter: «Vern av informasjon og informasjonsutveksling». I straffeloven fra 1902 lå mange av de tilsvarende bestemmelsene om datakriminalitet samlet under kapittelet «Forbrydelser mod den almindelige Orden og Fred.»

Straffeloven 2005 § 204 lyder:

«Med bot eller fengsel inntil 2 år straffes den som ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystem eller del av det.»

Den er tilsynelatende betydelig annerledes enn bestemmelsen om datainnbrudd i straffeloven fra 1902. Denne nye bestemmelsen heter «innbrudd i datasystem» og har blitt gitt en helt egen paragraf i straffeloven fra 2005.

Strafferammen er nå «bot eller fengsel inntil to år» og det er noen språklige forskjeller. I tillegg har det kommet et nytt vilkår om «brudd på beskyttelse eller annen uberettiget fremgangsmåte». Vilkåret om data som er «lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler» er tilsynelatende borte. Det samme gjelder det straffeskjerpende leddet som jeg gjennomgikk ovenfor.

9.1 Formål

Bestemmelsen fra 1902 hadde som formål å verne konfidensialitetshensynet, integritetshensynet og vederlagsinteressen. Se mer om disse i kapittel 7.1. I lovforarbeidene til den nye bestemmelsen blir det ikke nevnt noen endring i formålene og det er heller ikke noen grunn til å tro at formålene har blitt endret.

Det blir ikke lenger nevnt noe om data under overføring i bestemmelsen og det kan tenkes at dette kunne påvirke konfidensialitetshensynet. Konfidensialitetshensynet handler ikke *bare* om retten til privat kommunikasjon, men også om at (lagrede) data ikke skal blir gjort tilgjengelig for andre enn den berettigede. [42] Som jeg nevnte i kapittel 7.1 er det retten for den private omgang med elektronisk informasjon og tjenester som omfattes av konfidensialitetshensynet. Selv om

[42] NOU 2007: 2 s.51

bestemmelsen ikke lenger skulle omfatte data under overføring så vil dette altså ikke slå i hjel konfidensialitetsvernet den har for lagrede data.

9.2 Språklige forskjeller

Bestemmelsen fra 1902 bruker ordet *adgang* og den nye bestemmelsen bruker ordet *tilgang*. Det som er interessant er hvorfor dette ble endret og om det innebærer noen realitetsendring. I lovforarbeidene skriver justisdepartementet at *tilgang* er et mer dekkende ord. [42] Videre samsvarer det med strl. § 145 b (1902) og strl. § 201 (2005) som også bruker dette ordet. [43]

I bestemmelsen fra 1902 brukes ordene «data eller programutrustning», imens det i den nye bestemmelsen står «datasystem eller del av det». Justisdepartementet viser til at denne ordlyden samsvarer bedre med datakrimkonvensjonen og den finske datainnbruddsbestemmelsen. [43] De språklige forskjellene er ikke ment å innebære noen realitetsendringer. [43]

9.3 Vilkårene

9.3.1 Vilkår om beskyttelsesbrudd

Tidligere inneholdt datainnbruddsbestemmelsen et vilkår om beskyttelsesbrudd (bryte en beskyttelse eller på lignende måte). I 1985 skrev Datakrimutvalget i en utredning om datakriminalitet at:

«Tanken bak bestemmelsen er at det primært hviler på innehaveren av anlegget å sørge for beskyttelse mot innsyn fra uberettigede. Først når det er tatt rimelig foranstaltninger i så måte, kan han kreve hjelp fra strafferettsapparatet.» [44]

Vilkåret om beskyttelsesbrudd ble fjernet ved lovendring 8. april 2005 nr. 16. Begrunnelsen for dette lå i en høringsuttalelse fra Økokrim der det ble uttrykket et behov for å styrke vernet av data og datasystemer. [45] I en utredning fra 2007 skrev Datakrimutvalget at man fravek det prinsipielle utgangspunktet fra 1985-1987 da vilkåret om beskyttelsesbrudd ble fjernet. [46]

Selv om man ser at beskyttelsesbrudd blir nevnt i den nye bestemmelsen så innebærer ikke dette noen realitetsendringer. I bestemmelsen er det et vilkår om å skaffe seg tilgang ved å «bryte en

[43] Ot.prp.nr. 22 (2008-2009) s.403
[44] NOU 1985: 31 s.31
[45] Innst. O. nr. 53 (2004-2005) s.5
[46] NOU 2007: 2 s.48

beskyttelse eller ved annen uberettiget fremgangsmåte». Rettsstridsreservasjonen fra den gamle bestemmelsen er altså videreført. Beskyttelsesbrudd vil bare være et praktisk eksempel på en slik uberettiget fremgangsmåte. [47]

9.3.2 Vilkår om data eller programutrustning som er «lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler»

I den nye bestemmelsen har vilkåret om data som er «lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler» blitt fjernet. Justisdepartementet og flere av høringsinstansene uttalte at det å skaffe seg tilgang til data som overføres, og lagrede data, burde reguleres i forskjellige straffebud. [47] Begrunnelsen for dette var at disse forholdene har ulik karakter og at det samsvarer med datakrimkonvensjonens systematikk. [47]

I straffeloven fra 2005 beskyttes nå data som overføres i § 205 første ledd bokstav b. Bestemmelsen straffer den som uberettiget: «bryter en beskyttelse eller på annen uberettiget måte skaffer seg tilgang til informasjon som overføres ved elektroniske eller andre tekniske hjelpemidler».

I lovforarbeidene står det at denne bestemmelsen viderefører den delen av den strl. § 145 annet ledd (1902) som omhandler informasjon under overføring. [48] Den er altså et motsvar til bestemmelsen om innbrudd i datasystem i straffeloven fra 2005 som har et vern for lagret informasjon. [48]

9.4 Skyldkrav

Skyldkravet er forsett, jf. strl. § 22 (2005). Det følger av dekningsprinsippet at forsettet må dekke alle vilkår i gjerningsbeskrivelsen. Se kapittel 7.6 i oppgaven for mer om vilkårene opp i mot politiets etterforskning.

9.5 Strafferammen og straffeskjerpende omstendigheter

Tidligere i oppgaven gjennomgikk jeg strl. § 145 tredje ledd (1902). Et slikt straffeskjerpende ledd til datainnbruddsbestemmelsen finnes ikke i straffeloven fra 2005, men strafferammen har

[47] Ot.prp. nr. 22 (2008-2009) s.51
[48] Ot.prp. nr. 22 (2008-2009) s.404

blitt utvidet fra «bøter eller fengsel inntil 6 måneder eller begge deler» til «bot eller fengsel inntil to år».

Justisdepartementet har uttalt at denne utvidelsen av strafferammen innebærer enn oppjustering i forhold til gjeldende rett. [49] Dette er også mer på høyde med rett i andre nordiske land.

I tillegg skriver de at utvidelsen av strafferammen bl.a. er gjort med hensikt å dekke de alvorlige tilfellene og at det dermed ikke vil være nødvendig med en egen bestemmelse om grov overtredelse. [49] Det blir påpekt at innbrudd i datasystem fører til en form for skade, i motsetning til en forberedelseshandling. [49] Skadepotensialet og skadens omfang må vektlegges og det må bl.a. gjøres en vurdering av hva slags datasystem det er skaffet tilgang til. [50] Dersom det er et datasystem som inneholder personopplysninger eller andre sensitive opplysninger kan dette medføre stort skadepotensial, slik som vi så i Photobucket-dommen, Rt. 2012 s. 1968.

9.6 Oversikt over bestemmelsenes forskjeller

Formålet med den videreførte bestemmelsen er fortsatt det samme, selv om bestemmelsen har endret noe karakter. Den nye bestemmelsen inneholder noen språklige forskjeller som ikke innebærer noen realitetsendringer i forhold til gjeldende rett. Sentralt i begrunnelsene for endringene er harmonisering med andre bestemmelser.

Vilkåret om beskyttelsesbrudd medfører heller ikke noen realitetsendring fordi rettstridsreservasjonen også ble videreført. Videre har strafferammen blitt utvidet og oppjustert i den nye bestemmelsen. Skadepotensialet blir sett på som stort i saker om datainnbrudd. [51] Samtidig har noe av vurderingen i strl. § 145 tredje ledd (1902) blitt innbakt i den nye bestemmelsen, og den øvre delen av strafferammen er nok tiltenkt slike tilfeller.

Hovedforskjellen er at bestemmelsen i straffeloven fra 1902 omfattet både data som er lagret og som overføres, imens den nye bare omfatter lagrede data. Data som overføres er regulert som en egen bestemmelse i straffeloven § 205 første ledd bokstav b (2005). Dette er en egen paragraf om retten til privat kommunikasjon.

[49] Ot.prp. nr. 22 (2008-2009) s.51
[50] Ot.prp. nr. 22 (2008-2009) s.403
[51] Ot.prp. nr. 22 (2008-2009) s.403

10. Oppsummering

Forebygging av datakriminalitet er svært utfordrende. Dette gjelder også datainnbruddene, som spiller en sentral rolle innen datakriminaliteten. I en verden og et samfunn hvor utviklingen av informasjonsteknologi går lynkjapt er dette et tema som ikke er til å skyve under teppet. Samfunnskostnadene av datakriminaliteten er enorme. Mye tyder på at det finnes store mørketall og at risikoen for å bli oppdaget er forsvinnende liten.

Et viktig tiltak for å forebygge datakriminalitet er å styrke kunnskapene om datakriminaliteten, spesielt i politiet. Jeg håper at denne oppgaven kan være et bidrag til å øke kunnskapene om datakriminalitet, herunder datainnbrudd.

I denne oppgaven har jeg tolket strl. § 145 annet og tredje ledd, ved bruk av juridisk metode. Annet ledd er datainnbruddsbestemmelsen, og tredje ledd inneholder en utvidet strafferamme dersom noen straffeskjerpende momenter er til stede. Bestemmelsen verner konfidensialitetshensynet, integritetshensynet og vederlagsinteressen. Det er helt nødvendig å ha bestemmelser som verner disse godene.

Ikrafttredelsen av straffeloven 2005 er like rundt hjørnet. [52] I oppgaven tok jeg for meg forskjeller og ulikheter mellom datainnbruddsbestemmelsene i straffeloven fra 1902 og 2005. Mye er forandret på ordlyden og bestemmelsen i den nye straffeloven ser med første øyekast ganske ulik ut. Jeg kom i hovedsak frem til at den eneste realitetsendringen er at data som overføres ikke er omfattet av den nye bestemmelsen. I straffeloven fra 2005 er vernet for slik informasjon regulert i en annen paragraf som omhandler retten til privat kommunikasjon. Formålene med bestemmelsen i straffeloven fra 2005 er også de samme. Det er viktig at vernet om disse godene står sterkt i alle samfunn, og spesielt i samfunn hvor stadig mer forutsettes av, og hviler på, informasjonsteknologien.

[52] 1. oktober er foreslått i prop. 64 L (2014-2015) s.7

Litteratur

Pensum

Lie, E. M. (2011). *I forkant: Kriminalitetsforebyggende politiarbeid*. Oslo: Gyldendal akademisk.

Selvvalgt pensum

Datakriminalitet: Hva er datakriminalitet? (sist oppdatert 09. februar 2015) Hentet april 2015 fra politiets internettsider: https://www.politi.no/kripos/datakriminalitet/

Datasnok (sist endret 12. april 2015). Hentet april 2015 fra Wikipedias internettsider: http://no.wikipedia.org/wiki/Datasnok

Den europeiske menneskerettighetskonvensjonen (1950). Hentet april 2015 fra: https://lovdata.no/dokument/NL/lov/1999-05-21-30/KAPITTEL_2#KAPITTEL_2

Nasjonal Sikkerhetsmyndighet (2011). *Rapport om sikkerhetstilstanden.* Hentet april 2015 fra: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2011.pdf

Næringslivets Sikkerhetsråd (2012). *Mørketallsundersøkelsen: Informasjonssikkerhet og datakriminalitet*. Hentet april 2015 fra: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/moerketall_2012.pdf

Storruste, B. L. (2014). *Datakriminalitet.* Oslo: Politihøgskolens trykkeri

Sunde, I. M. (2006). *Lov og rett i cyberspace.* Oslo: Fagbokforlaget Vigmostad & Bjørke AS

Økt innsats mot datakriminalitet (sist oppdatert 27. januar 2012). Hentet april 2015 fra politiets internettsider: https://www.politi.no/kripos/aktuelt/nyhetsarkiv/2012_01/Nyhet_10916.xml

Lover

Menneskerettsloven (1999). *Lov av 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett med endringer, sist ved lov av 09. mai 2014 nr. 14 (i kraft samme dag).* Hentet april 2015 fra: http://www.lovdata.no/all/hl-19950804-053.html

Politiloven (1995). *Lov av 4. august 1995 nr. 53 om politiet med endringer, sist ved lov av 20. juni 2014 nr. 47 (i kraft 1. juli 2014).* Hentet april 2015 fra: http://www.lovdata.no/all/hl-19950804-053.html

Straffeloven (1902). *Lov av 22. mai 1902 nr. 10 almindelig borgerlig straffelov med endringer, sist ved lov av 24. april 2015 nr. 22 (i kraft 1. mai 2015).* Hentet mai 2015 fra: https://lovdata.no/dokument/NL/lov/1902-05-22-10?q=straffeloven

Straffeloven (2005). *Lov av 20. mai 2005 nr. 28 om straff med endringer, sist ved lov av 20. juni 2014 nr. 49 (i kraft 1. juli 2014).* Hentet mai 2015 fra: https://lovdata.no/dokument/NL/lov/1902-05-22-10?q=straffeloven

Offentlige publikasjoner

Innst. O. nr. 53 (2004-2005). Lovtiltak mot datakriminalitet. Hentet april 2015 fra: https://www.stortinget.no/globalassets/pdf/innstillinger/odelstinget/2004-2005/inno-200405-053.pdf

NOU 1985: 31. Datakriminalitet. Hentet april 2015 fra: http://www.nb.no/nbsok/nb/da51470e89a0eecc155102a166e3738e.nbdigital?lang=no#0

NOU 2003: 27. Lovtiltak mot datakriminalitet. Hentet april 2015 fra: https://www.regjeringen.no/contentassets/9842026befcd4bff8d3993292e23f3e3/no/pdfs/nou200320030027000dddpdfs.pdf

NOU 2007: 2. Lovtiltak mot datakriminalitet. Hentet april 2015 fra: https://www.regjeringen.no/contentassets/4416e850ad5e4e45b112e21c74e5332d/no/pdfs/nou200720070002000dddpdfs.pdf

Ot.prp.nr.4 (1978-1979). Om lov om endringer i straffeloven. Hentet april 2015 fra: https://lovdata.no/pro/#document/PROP/forarbeid/otprp-4-197879

Ot.prp.nr.35 (1986-1987). Om endringer i straffeloven (datakriminalitet). Hentet april 2015 fra: https://lovdata.no/pro/#document/PROP/forarbeid/otprp-35-198687

Ot.prp.nr.40 (2004-2005). Lovtiltak mot datakriminalitet. Hentet april 2015 fra: https://www.regjeringen.no/contentassets/4deac3823b2f48cc9d7b2d5a2d9091f3/no/pdfs/otp200420050040000dddpdfs.pdf

Ot.prp. nr. 22 (2008-2009). Om lov om endringer i straffeloven 20. mai 2005 nr. 28. Hentet april 2015 fra: https://www.regjeringen.no/contentassets/10118c83df37474e9c61e86765c7af98/no/pdfs/otp200820090022000dddpdfs.pdf

Prop. 64 L (2014-2015). Lov om ikraftsetting av straffeloven 2005. Hentet april 2015 fra: https://www.regjeringen.no/contentassets/77da96f2e3064b7798702b56a1d2ac31/no/pdfs/prp201420150064000dddpdfs.pdf

Domsoversikt

Frostating lagmannsrett, RG. 2010 s. 618	LF-2009-202167
Høyesterett, Rt. 1994 s. 1610	HR-1994-179-B
Høyesterett, Rt. 1995 s. 35 (Smartkort-dommen)	HR-1995-2-A
Høyesterett, Rt. 2004 s. 94	HR-2004-127-A
Høyesterett, Rt. 2012 s. 1968 (Photobucket-dommen)	HR-2012-2056-A
Høyesterett, Rt. 2012 s. 1669	HR-2012-2397-A