Sitering av artikkelen i APA (6th):
Sunde, i. M. (2019). Har vi behov for straffebud om datakriminalitet?. *Tidsskrift for strafferett*, *19*(2), 168-185.

Har vi behov for straffebud om datakriminalitet?[1]

Professor Inger Marie Sunde, Politihøgskolen.

Inger Marie Sunde er professor i rettsvitenskap ved Politihøgskolen i Oslo og leder forskergruppen Politiet i et digitalisert samfunn. Hun var sekretær og medlem av Datakrimutvalget I og II, har utgitt fagbøkene *Lov og rett i cyberspace* (2006) og *Datakriminalitet* (2016), og publisert artikler om datakriminalitet, politiets digitale metodebruk, personvern og overvåking.
ingsun@phs.no

Sammendrag

Artikkelen analyserer gjerningsbeskrivelsen i straffebud om datakriminalitet. Det går et skille mellom ytrings- og handlingsstraffebud som er relevant for lovbrudd på internett, og straffebudene burde i større grad reflektere dette. Av hensyn til legalitetsprinsippet og behovet for en rimelig tilgjengelig og klar straffelov foreslås det også visse forenklinger. I dagens utforming er straffebudene vanskelige å forstå, og de er heller ikke helt dekkende for det de er ment å ramme. Flere forskjellige lovbrudd tar utgangspunkt i krenkelse av datasikkerheten, og beskrivelsen av denne modusen burde konsentreres til ett sted. De forskjellige etterfølgende moduser kunne utpensles i umiddelbar tilknytning til dette (databedrageri, dataskadeverk, datainnbrudd, ulovlig overvåking, driftshindring). I lys av datateknologiens store utbredelse kan en rekke tradisjonelle lovbrudd dessuten begås ved å manipulere datasystemer. Spørsmålet gjelder behovet for å straffe datalovbruddet i konkurrens med det tradisjonelle lovbruddet. En mulighet kan være heller å gjøre det tradisjonelle lovbruddets dataaspekt til en generell straffskjerpende omstendighet. Dette vil kunne lette etterforskningen og effektivisere strafforfølgningen.

Nøkkelord: datakrim, databedrageri, dataskadeverk, datainnbrudd, ulovlig overvåking, tingenes internett

1. Datakrimstraffebudene gjenspeiler teknologien på 1990-tallet

Straffebud består av to hovedelementer: den objektive gjerningsbeskrivelsen og skyldkravet (gjerningspersonens kunnskap om den faktiske situasjonen). Artikkelen gjelder

[1] Dette er et opptrykk av min artikkel inntatt i *I forskningens og formidlingens tjeneste – festskrift til professor Lars Bo Langsted*, Bønsing, S., Elholm, T., Jakobsen, S.S. og Lentz, L.W. (red.), kapittel 20, s. 329–325, ExTuto Publishing, København 2018. Opptrykket er gjort med velvillig tillatelse fra redaktørene og ExTuto Forlag. Jeg har gjort to tilføyelser i brødteksten (markert med klammeparentes), og tilføyelser i fotnote 11, 29, 31, 40, 43 og 45 (også markert med klammeparentes). Flere av endringene skyldes avløsningen av åndsverkloven fra 1961 med lov om åndsverk 15. juni 2018 nr. 40.

gjerningsbeskrivelsen *i straffebud om datakriminalitet*. Fokus rettes mot forbrytelsens eksterne (objektive) kjennetegn slik de er beskrevet i straffebudet.

Norge har gjennomført Europarådets datakrimkonvensjon fra 2001, herunder sørget for å kriminalisere forbrytelsene som er regnet opp i konvensjonen artiklene 2 til 10.[2] Forbrytelsene som dermed er tatt inn i straffeloven, er utformet som *spesielle bestemmelser om datakriminalitet*.[3] Gjerningsbeskrivelsen er dataspesifikt utformet ved å inneholde ord som «datasystem», «data» eller beslektede formuleringer. Slik ordlyd er benyttet i straffeloven § 201 (uberettiget befatning med passord og hackerverktøy), § 204 (innbrudd i datasystem), § 205 bokstav b (uberettiget tilgang til elektronisk informasjon som overføres), § 206 (fare for hindring av driften av et datasystem), § 351 annet ledd (dataskadeverk), § 361 annet ledd (elektronisk dokument) og § 371 bokstav b (databedrageri). Bestemmelsene gjennomfører Datakrimkonvensjonen artikkel 2 til 6 (krenkelser av data og datasystemer), artikkel 7 (datarelatert dokumentfalsk) og artikkel 8 (databedrageri).

Den dataspesifikke utformingen avviker fra den tradisjonelle preferansen for «syntetisk lovgivning» i strafferetten.[4] «Syntetisk» kan forstås som motsatsen til «kasuistisk» eller «spesiell». I den syntetiske tradisjonen er gjerningsbeskrivelsen utformet med bruk av ord og uttrykk på ganske generelt nivå. Det gir straffebud som er fleksible og holdbare over tid, fordi de er anvendelige på nye fenomener så vel som på de som eksisterte da straffebudet ble til. Interessant nok er straffeloven § 311 (forbud mot befatning med overgrepsbilder av barn) syntetisk utformet. Straffebudet gjennomfører Datakrimkonvensjonen artikkel 9 som forbyr slik befatning når det skjer *ved bruk av et datasystem*. Det til tross nevner § 311 verken data eller datasystem. Forskjellen mellom § 311 og de andre bestemmelsene som er nevnt, har inspirert denne artikkelen.[5]

Datakrimstraffebudene fremstår etter min mening som mindre treffende for dagens forhold. Den omfattende utbredelsen av «det digitale» – den digitale integreringen i alle ting og individer – gjør det vanskelig å trekke grenser mellom det som er å anse som et «datasystem», og det som er «ting» integrert som komponenter i datasystemene. Dette har rettslige konsekvenser. Det har også den pågående transformasjonen av tradisjonelle objekter som regelrett blir til datasystemer. Biler – de selvkjørende så vel som de som fremdeles har en sjåfør bak rattet – er et eksempel på dette; telefonen som har blitt «smart», er et annet.

I tillegg til å gjennomføre kriminaliseringsforpliktelsen etter Datakrimkonvensjonen har datakrimstraffebudene til formål å verne informasjon i vid forstand, uavhengig av om den er i

[2] Europarådets konvensjon om datakriminalitet av 23.11 2001 (CETS 185). Den nasjonale implementeringen ble forberedt i delutredningene *Lovtiltak mot datakriminalitet* (NOU 2002: 27 og 2007: 2). Lovproposisjonene er Ot.prp. nr. 40 (2004–2005) og nr. 22 (2008–2009).

[3] Straffeloven er lov om straff av 20. mai 2005 nr. 28. Loven trådte i kraft 1. oktober 2015.

[4] Se Tor-Geir Myhrer, «Ny straffelov», *Jussens Venner* 2/2008, s. 95–135, s. 112–113.

[5] Konvensjonen artikkel 10 som verner opphavsrettigheter og nærstående rettigheter, er gjennomført via straffehjemmelen i åndsverkloven § 54 (lov om opphavsrett til åndsverk mv. av 12. mai 1961 nr. 2). Krenkelse av slike rettigheter behandles ikke her.

digital eller annen form. Bredden i beskyttelsen gjør fokuset utydelig. Den enkelte bestemmelses formål blir ytterligere diffus når det tas i betraktning at datateknologien innvirker på de fleste beskyttelsesverdige interesser, på så vel individ- som samfunnsplan. Skal for eksempel § 204 (datainnbrudd) først og fremst verne datasystemer? Eller skal den primært verne privatlivsinteresser mot uønsket eksponering, alternativt beskytte kommersielle og offentlige behov for konfidensialitet og uforstyrret drift? Skal § 351 annet ledd primært verne data som digitalt formuesgode, på linje med fysiske objekter? Eller er det borgernes behov for fungerende systemer som vernes?

Problemene kan ha flere årsaker, blant annet at lovgiver har søkt å henføre for mange ulike interesser under bestemmelsene. En annen grunn er også tenkelig, nemlig at datakrimstraffebudene reflekterer teknologistadiet på slutten av 1990-tallet. På den tiden ble et datasystem forstått som å være *en avgrenset fysisk innretning som hadde databehandling som sitt endelige formål.* I dag kan et datasystem knapt skilles fra et nettverk eller fra en ting. Dessuten er data blitt et råstoff, ofte kun behandlet som *et middel for å kunne yte en tjeneste eller få et objekt til å utføre en funksjon* (tenk på en «fitbit»). Det som således burde fange oppmerksomheten, er at det meste er i ferd med å bli (del av) et datasystem, noe eksemplene nedenfor kan illustrere:

> (i) En nettverksbasert blodsukkermåler/pacemaker settes ut av funksjon ved å forstyrre nettverksforbindelsen. Brukeren (pasienten) påføres skade/dør. (ii) En hund trenes med hjelp av lydsignaler fra en innretning på halsbåndet. Innretningen er koblet til en mobilapplikasjon. Mobilapplikasjonen ødelegges av en hacker slik at lydsignalene avgis helt tilfeldig. Hunden utsettes dermed for alvorlig stress. (iii) En gammel arvetante gjør bruk av ny velferdsteknologi som forteller når hun skal ta hjertemedisinen sin. Den datakyndige nevøen manipulerer systemet slik at hun overdoserer og dør. (iv) Datastyrt dørlås er en tjeneste som kan kjøpes av et foretak. En hacker bryter seg inn i foretakets datasystem og låser opp kundenes dørlåser. (v) En Tesla kan anses som et datasystem utstyrt med de nødvendige egenskaper til å fungere som en bil. Teslaen kolliderer fordi en hacker har tuklet med navigasjonssystemet. (vi) I nær fremtid kommer biler til å respondere automatisk på signaler i sanntid fra et nasjonalt system for trafikksikkerhet. Ved kødannelse og eventuell bråstopp slår bremsene automatisk inn. Et angrep på systemet forårsaker en stor kjedekollisjon.

Bedømt etter *gjerningens resultat* gjelder eksemplene tradisjonell kroppskrenkelse, dyremishandling, drap, skadeverk og angrep på infrastrukturen. Dette er straffbart etter tradisjonelle straffebud. Spørsmålet er om det er vesentlig å straffe for datainnbruddet/-skadeverket *i tillegg,* slik datakrimbestemmelsene legger opp til.

Datakrimkonvensjonen tar naturligvis ikke hensyn til utviklingstrekk som har skjedd etter at den ble til. Dette søkes kompensert gjennom veiledende noter som behandler nye strafferettslige problemstillinger etter hvert som de dukker opp.[6] Men uansett er

[6] I skrivende stund (juli 2017) foreligger 11 veiledende noter utferdiget av Europarådets Cybercrime Convention Committee (T-CY). Notene er tilgjengelige på http://www.coe.int/en/web/cybercrime/guidance-notes.

konvensjonen et produkt av 1990-tallets teknologiske forståelsesramme (ekspertgruppen som laget konvensjonsutkastet, startet arbeidet i 1997). Fra 2001, da konvensjonen ble undertegnet, har datautviklingen akselerert, og datautstyr, sosiale medier, bredbånd og mobilapplikasjoner har blitt del av dagliglivet. Tingenes internett er integrert i våre omgivelser, til dels med oss selv som tilkoblete «ting». Kunstig intelligens, roboter og delingsøkonomi dominerer i medieoverskriftene.[7] Verden ser følgelig annerledes ut enn i 2001. Det kan tale for at loven bør se annerledes ut.

2. Opplegg for analysen

Datautviklingen har satt sine spor i strafferetten også *uavhengig av Datakrimkonvensjonen.* Kapittel 3 redegjør for tre tilfeller av slik teknisk innflytelse hvor loven har fanget opp negative sider av teknologiutviklingen uten behov for dataspesifikke bestemmelser. Dette er en rettslig fleksibilitet som går på siden av Datakrimkonvensjonens kasuistikk. Analysen utdypes i kapittel 4 som tar opp lovtolking relatert til en digital faktisk kontekst. Analysen trekker veksler på sondringen mellom ytringer og handlinger. Kapittel 5 vender tilbake til tingenes internett og eksemplene nevnt i kapittel 1. Det avsluttende kapittel 6 reiser noen rettspolitiske spørsmål om data*sikkerhets*kriminalitet versus annen kriminalitet.

Det tas ikke hensyn til spesielle grunner for å ha dataspesifikke straffebud, f.eks. å lette internasjonal kontroll med gjennomføring av konvensjonsforpliktelser.[8] Siden siktemålet nettopp er *å belyse et mulig behov for endring*, faller slike aspekter utenfor artikkelens ramme.

Paragrafhenvisningene gjelder den nye straffeloven,[9] noe som er presisert med «strl.» når det er nødvendig for å unngå uklarhet. Henvisninger til den gamle straffeloven fra 1902 er gjort med forkortelsen «gstrl.» foran paragraftegnet.[10]

3. Datautviklingen som strafferettslig påvirkningsfaktor

Digitaliseringen har slått inn i strafferetten på langt bredere front enn reflektert i Datakrimkonvensjonen. I noen tilfeller har straffeloven blitt endret eller supplert for å ramme digitale handlemåter på lik linje med andre overtredelsesmåter. Det har ikke vært nødvendig å benytte dataspesifikk utforming for å oppnå dette. Videre har det skjedd en utvikling i synet på privatlivskrenkelser som begås digitalt. Utviklingen har skjedd i rettspraksis og er begrunnet i spesielle egenskaper ved det digitale. Sakene gjelder imidlertid overtredelse av tradisjonelle straffebud.

---

[7] For å minne om at den alminnelige internettbruken har kort historie, nevner jeg at sosiale medier kom ca. 2005 (Facebook i 2004), og at mobilapplikasjonene inntok mobiltelefonene ca. 2010. Omtrent samtidig kom strømmetjenester som Spotify, og kryptovaluta som Bitcoin.

[8] Hensynet har vært tillagt betydning i arbeidet med den nye straffeloven. Se Myhrer, op.cit., fn. 4.

[9] Ibid., fn. 3.

[10] Alminnelig borgerlig straffelov av 22. mai 1902 nr. 10. Den gamle straffeloven gjaldt frem til 1. oktober 2015 da den nye straffeloven trådte i kraft.

3.1 Straffbare ytringer på internett

Enkelte ytringer er straffbare såfremt de er offentlig fremsatt. Det gjelder blant annet oppfordring til å iverksette terrorhandling (§ 136 bokstav a) eller annen straffbar handling (§ 183), hatefulle ytringer (§ 185), ytring som krenker privatlivets fred (§ 267), og publisering av personfoto uten avbildetes samtykke (åndsverkloven § 45c, jf. § 54).[11] Strafforfølgning av slike ytringer publisert på internett har imidlertid voldt atskillig rettslig hodebry på grunn av vilkåret «offentlig», jf. legaldefinisjonen i gstrl. § 7.

Problemet gjaldt ytringer fremsatt på nettsteder som brukerne kontakter individuelt i ettertid. Ingen av alternativene i den gamle legaldefinisjonen var da anvendelige. Legaldefinisjonen lød:

> «En Handling ansees forøvet offentlig, naar den er forøvet ved Udgivelse af trykt Skrift eller i Overvær af et større Antal Personer eller under saadanne Omstendigheder, at den let kunde iakttages fra et offentlig Sted og er iagttaget af nogen der eller i Nærheden værende».

Første alternativ var utelukket fordi informasjon på internett ikke har vært ansett som «trykt skrift».[12] Annet alternativ var utelukket fordi vilkåret «i overvær av» krever samtidighet, dvs. at ytringen må mottas av adressatene idet den fremsettes. Tredje alternativ var utelukket fordi internett ikke regnes som «offentlig sted». Lovforståelsen er senest bekreftet i HR-2016-1458-A (Haxi). Transporttjenesten Haxi ble frembudt via en mobilapplikasjon. Taxitjeneste er underlagt løyveplikt såfremt tjenesten rettes til allmennheten på «offentlig plass» (sml. «offentlig sted»). Siden mobilapplikasjonen ble ikke ansett som offentlig sted, forelå heller ikke rettslig grunnlag for å straffe tilbud om Haxi-transport uten løyve.

Tolkingen har sett bort fra om nettstedet er allment tilgjengelig eller faktisk har mange besøk. Den strenge tolkningspraksisen føyer seg inn i innskjerpingen av legalitetsprinsippet siden 2009.[13] Behovet for å kunne slå ned på slike ytringer ble imidlertid stadig mer påtakelig, særlig på grunn av den utbredte forekomsten av hatefulle og ekstremistiske ytringer.[14] Det oppsto også et spenningsforhold til vilkåret «et større antall personer», som bare krevde at ytringen

---

[11] [Tilføyelse i opptrykk: Bestemmelsen er videreført i § 104 i åndsverkloven av 15. juni 2018 nr. 40 som trådte i kraft 1. juli samme år. Den eldre åndsverkloven ble samtidig opphevet.] Unntak fra samtykkekravet fremgår av § 45c bokstav a–e. Bokstavene a–c nevner omstendigheter hvor personvernet viker for ytringsfriheten. Bokstavene d og e gjelder fotografens rettigheter.

[12] Jon Bing, *Ansvar for ytringer på nett* (Universitetsforlaget, Oslo 2008), kapittel 5.2.1, tok til orde for at *muligheten* for at et større antall personer kan fremstille fysisk eksemplar av et skrift som er tilgjengeliggjort på internett, bør være tilstrekkelig til å oppfylle legaldefinisjonen. Se også mindretallet i Rt. 2012 s. 1211 (blogg).

[13] Det strafferettslige lovskravet følger av Grunnloven § 96, EMK artikkel 7 og strl. § 14. Skjerpingen er belyst av Arnfinn Bårdsen, «Grunnloven, straffeprosessen og strafferetten – noen linjer i høyesteretts praksis etter grunnlovsreformen 2014», *Jussens Venner* 1/2017, s. 1–44. Se også Thomas Frøberg, «Nyere praksis om det strafferettslige legalitetsprinsippet», *Jussens Venner* 01-02/2015, s. 46–71.

[14] Inger Marie Sunde (red.), *Forebygging av radikalisering og voldelig ekstremisme på internett*. PHS Forskning nr. 1/2013. Politihøgskolen, Oslo.

nådde 20–30 personer.[15] Vilkåret er lett oppfylt på internett hvor vennekretsen i sosiale medier kan måle hundretalls, og utallige mekanismer for viderespredning gjør det nærmest umulig å forbeholde informasjon for en begrenset krets.[16] At ytringene likevel ikke var å anse som «offentlig» fremsatt, var åpenbart en svakhet.

Etter Rt. 2012 s. 1211 (blogg) kunne moderniseringen av loven ikke lenger utsettes. Politiet hadde begjært varetektsfengsling av en mann som på bloggen sin hadde oppfordret til drap på polititjenestemenn. Bedømt etter innholdet var ytringene utvilsomt straffbare, jf. gstrl. § 140 (nå § 183). Spørsmålet var om oppfordringen var offentlig fremsatt. Bloggen var allment tilgjengelig, og siktede opplyste å ha hatt totalt ca. 70 000 treff og 50 lesere daglig.[17] Høyesteretts flertall (ankeutvalget) fant imidlertid at vilkåret «offentlig» ikke var oppfylt. Oppfordringen oppfylte dermed ikke gjerningsbeskrivelsen, og grunnlag for varetektsfengsling forelå ikke.

Etter dette ble legaldefinisjonen i strl. § 10 forskuttert iverksatt i gstrl. § 7.[18] Den nye legaldefinisjonen gjør *publiseringsmåten* til det avgjørende kriterium, nemlig hvorvidt ytringen er fremsatt på en måte som gjør den «egnet til å nå» et større antall personer.[19] Om et nettsted er et lukket forum, er uten betydning såfremt antallet medlemmer er tilstrekkelig høyt. En hatefull ytring postet på den lukkede Facebook-gruppen Profetens Ummah ble således ansett å være offentlig siden gruppen hadde ca. 3000 medlemmer. Det hadde ikke betydning at det var usikkert hvor mange som hadde sett den, eller at den var blitt slettet etter 20–30 minutter.[20]

Merk at formålet med å endre legaldefinisjonen var å sørge for at *ytringsstraffebudene også rammet ytringer på internett.* Utformingen er likevel ikke dataspesifikk, jf. «egnet til å nå».

3.2 Identitetskrenkelse

Selv om misbruk av en annens identitet neppe noen gang har vært ansett som redelig og korrekt oppførsel, har det ikke vært en straffbar handling i seg selv. Loven har heller rammet indirekte, f.eks. når misbruket har skjedd som ledd i bedrageri eller dokumentfalsk. Etter omstendighetene kunne også gstrl. § 390a (nå § 266) være aktuell. Bestemmelsen straffer hensynsløs atferd som krenker en annens fred.

---

[15] Ot.prp. nr. 90 (2003–2004) s. 187 og 408–409. Selv om 20–30 personer har etablert seg som norm, har det vært fundert over om kravet burde nyanseres i lys av den konkrete situasjonen. Se Ellen Lexerød Hovlid, «Straffelovens definisjon av en 'offentlig handling'», *Tidsskrift for strafferett* 02/2016, s. 161–181; Inger Marie Sunde, *Datakriminalitet* (Fagbokforlaget, Bergen 2016), kapittel 3.2.

[16] Jeg har behandlet spredningstemaet nærmere i relasjon til personvernet, se Sunde, *Automatisert innhentning*, doktoravhandling (ph.d.) nr. 37 ved juridisk fakultet, Oslo, 2010 (Complex nr. 3/2011 Unipub, Oslo); «Økosystemeffekten – om personvernet i sosiale medier», *Lov og Rett* 01/2013, s. 85–102; og *Datakriminalitet*, op.cit., fn. 15, kapittel 10.

[17] Lagmannsrettens kjennelse, LG-2012-119111 (Gulating).

[18] Endringslov 24. mai 2013 nr. 18. Prop. 53 L (2012–2013), Innst. 221 L (2012–2013).

[19] Ot.prp. nr. 90 (2003–2004) s. 187 og s. 408–409.

[20] LB-2014-174730 (Borgarting). Dommen gjaldt gstrl. § 135a (nå § 185).

Ved inngangen til det nye årtusen vokste det frem en erkjennelse av at identitetskrenkelse var blitt et stort og alvorlig problem. Årsaken ble først og fremst tilskrevet datautviklingen. Det ledet til konklusjonen om at det var behov for en ny straffebestemmelse som rammet identitetskrenkelse (heretter «ID-krenkelse») som selvstendig forbrytelse, jf. § 202.[21] Gjerningsbeskrivelsen rammer den som uberettiget «opptrer med en annens identitet eller med en identitet som er lett å forveksle med en annens identitet».[22]

Den legislative begrunnelsen er sammensatt. Først og fremst ble offerets behov for beskyttelse fremhevet. Misbruk av identitet kan ha negative konsekvenser både for omdømme og økonomi, og store anstrengelser kan være nødvendige for å rydde opp i situasjonen. Videre er det lagt vekt på at identitetsinnehaveren har små muligheter for å beskytte seg. Offeret rammes typisk tilfeldig som følge av at personopplysninger er kommet på avveie. De kan f.eks. stamme fra en database som har vært gjenstand for datainnbrudd. Det var derfor behov for å oppnå en generell allmennpreventiv effekt gjennom straffetrussel. Sist, men ikke minst ble betydningen av å kunne stole på nettbaserte tjenester understreket. Tjenester som er avhengig av identitetsopplysninger, kan bare ha fremgang dersom man kan ha tillit til informasjonen som avgis. Tillitshensynet overfor digitale tjenester forklarer hvorfor § 202 er plassert i kapittel 21 «Vern av informasjon og informasjonsutveksling» sammen med flere dataspesifikke straffebud som verner datasikkerheten (§ 201, § 204, § 205 bokstav b, § 206). Privatlivskrenkelsen hadde ellers talt for plassering i kapittel 24 «Vern av den personlige fred og frihet».

ID-krenkelse (eventuelt «ID-tyveri») har ikke noen bestemmelse i Datakrimkonvensjonen, men er behandlet i veiledende note nr. 4.[23] Her sies det at «ID-tyveri rammer statlige myndigheter, foretak og borgerne og forårsaker stor skade. Det undergraver tiltro og tillit til informasjonsteknologien» (min oversettelse fra engelsk). Noten belyser deretter hvordan ID-tyveri kan være et element i datakrimforbrytelsene som er regnet opp i konvensjonen.

Som nevnt kan identitetsmisbruk inngå som ledd i bedrageri. Mens man tidligere kun straffet for bedrageriet, har innføringen av § 202 redefinert handlingen til å utgjøre to forbrytelser. Nå skal det straffes etter § 202 i idealkonkurrens med § 371 bokstav a (bedrageri), noe som skal lede til straffskjerpelse, jf. § 79 bokstav a. Identitetsinnehaveren har status som fornærmet på linje med offeret for bedrageriet.

---

[21] Ot.prp. nr. 22 (2008–2009) s. 44 f. Bestemmelsen ble forskuttert innført i gstrl. § 190a ved lovendring 10. desember 2010 nr. 73. Prop. 14 L (2010–2011).

[22] Gjerningsbeskrivelsen for ID-krenkelse står i § 202 annet og tredje alternativ. Første alternativ rammer den som «uberettiget setter seg i besittelse av en annens identitetsbevis». Det at straffebudet rammer flere forskjellige handlinger og verner en rekke forskjellige interesser (dokumentsikkerhet, identitetssikkerhet og nettsikkerhet), gjør den kompleks og vanskelig tilgjengelig. Bestemmelsen er behandlet i Sunde, *Datakriminalitet*, op.cit., fn. 15, kapittel 8.

[23] Guidance Note 4 *Identity theft and phishing in relation to fraud* (T-CY (2013) 8E Rev).

For analysen har det betydning at det sentrale vilkåret «opptrer» skal tolkes slik at det gjelder *overfor et annet menneske*.[24] Dette skiller ID-krenkelse fra rettsstridig autentisering overfor et datasystem (passordinnbrudd). Avgivelse av passord til et datasystem verifiserer brukeridentiteten. Bruk av stjålet passord anses imidlertid ikke som å «opptre», jf. § 202, siden mottakeren (datasystemet) ikke er et menneske. Derimot omfattes *phishing,* f.eks. opprettelse av falske websider som utnytter omdømmet til velrenommerte foretak. Overtredelsen begås da ved kommunikasjon overfor mennesker.

Til sist bør man merke seg at til tross for at digitaliseringen lå bak behovet for det nye straffebudet, unngikk lovgiver bruk av dataspesifikk gjerningsbeskrivelse. Ifølge forarbeidene gjelder bestemmelsen «uavhengig av om utnyttelsen av en annens identitet skjer ved hjelp av elektronisk utstyr eller på annen måte, for eksempel i bankskranken eller per brev».[25]

3.3 Evighetsaspektet ved digitale personvernkrenkelser

Rettsstridig publisering av privat eller personlig informasjon skjer i betydelig omfang, og problemet er særlig assosiert med publisering av personfoto. Det har vært lagt vekt på at egenskaper ved det digitale medfører at personvernkrenkelsen blir mer graverende enn før. Omfattende viderespredning gjør materialet vedvarende tilgjengelig på internett. Når materialet først er viderespredt, lar ytterligere spredning seg ikke begrense eller kontrollere.[26] I Rt. 2002 s. 1187 trakk Høyesterett opp retningslinjer for straffutmåling for ulovlig befatning med overgrepsbilder av barn (nå strl. § 311),[27] og førstvoterende uttalte med tilslutning fra de øvrige dommerne:

> «I tillegg til den enorme spredning som oppnås ved å legge bilder ut på Internett, er det i praksis ikke mulig å få slettet dem. Barn som er blitt misbrukt gjennom produksjon av pornografi, vil således oppleve å kunne bli gjenkjent i årevis. Det dreier seg i slike tilfeller om en livsvarig krenkelse, som aktor ganske treffende uttrykte det. Man må regne med at risikoen for at andre kommer over bildene vil være en betydelig tilleggsbelastning senere i livet for den det gjelder» (s. 1191).

Den evige integritetskrenkelsen er også kommet til uttrykk når det gjelder bilder som er tatt frivillig, blant annet «selfies», når slike er kommet på avveie. En dom fra 2016 (HR-2016-2263-A) gjaldt straffutmåling ved domfellelse for heleri, jf. gstrl. § 317 (nå § 332). Utbyttet besto i 36 270 Snapchat-bilder som domfelte hadde lastet ned fra internett.[28] De fleste bildene viste jenter på ca. 18 år. For 200 av jentene hadde domfelte systematisert bildene på mapper med

[24] Ot.prp. nr. 22 (2008–2009) s. 45.
[25] Ot.prp. nr. 22 (2008–2009) s. 21.
[26] Se Sunde, *Økosystemeffekten*, op.cit., fn. 16.
[27] Saken gjaldt gstrl. § 211, senere gstrl. § 204 a. Bestemmelsen er videreført i strl. § 311. Betegnelsen «overgrepsbilder» beskriver at bildene dokumenterer seksuelle overgrep. Dessuten er filmingen og spredningen overgrep mot barnets personvern; «*The Luxembourg Guidelines*», *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Adopted by the Interagency Working Group in Luxembourg, 28.1.16. (Section F).
[28] Informasjon som har verdi, økonomisk eller på annet vis, omfattes av ordet «utbytte» i straffebudet.

navn og adresse. Domfelte var klar over at de fornærmede ikke hadde samtykket til spredningen på internett. Den forutgående forbrytelsen gjaldt således overtredelse av åndsverkloven § 45c, jf. § 54.[29]

Høyesterett konstaterte at retten til kontroll med eget fotografi «har en klar side til personvernet» (avsnitt 16), og sa at det er «i seg selv en stor integritetskrenkelse at slike bilder kommer på avveier. Enda mer alvorlig blir det når man blir identifisert med navn og bosted. Bildene kan potensielt bli fanget opp av venner og kjente, familie og naboer og ikke minst av nåværende eller potensiell arbeidsgiver» (avsnitt 18). Endelig ble det konstatert at det er «svært vanskelig å få slettet bilder fra nettet, og den manglende kontrollen med hvor bildene befinner seg, kan gjøre dette til en nærmest livslang krenkelse for de berørte» (avsnitt 19).

Bruk av kamerafunksjonen på smarttelefonen og påfølgende tilgjengeliggjøring i sosiale medier er kilde til alvorlige privatlivskrenkelser. En tingrettsdom som fikk medieoppmerksomhet i juni 2017, gjaldt et ungt par (begge under 18 år) som ble fotografert mens de hadde samleie på badet under en fest. Fotografen – en mannlig festdeltaker med en iPhone – la ut bildene på en Snapchat-funksjon (MyStory) som tilgjengeliggjør bildene for alle Snapchat-vennene. Etter oppfordring fra noen festdeltakere fjernet han bildene etter 15 minutter, men da var de alt viderespredt, «og dette fortsatte i ukene som fulgte».[30] Han ble anmeldt av piken på bildet og domfelt etter § 266 om hensynsløs atferd som forstyrrer en annens fred. I forbindelse med straffutmålingen viser retten til sitatet i høyesterettsavgjørelsen fra 2002, dvs. den digitale evighetskrenkelsen. Straffebudene (åvl. § 45c, jf. § 54 og gstrl. § 317) nevner imidlertid verken data eller datasystem.

Den evige integritetskrenkelsen er en konsekvens av teknologiutviklingen. Effekten på personvernet er klarligvis relevant for straffebud som uttrykkelig gjelder personvernet, slik som § 267 (privatlivets fred) og åndsverkloven § 45 c, jf. § 54 (retten til eget bilde).[31] Vel så interessant er det at evighetsaspektet også trekkes frem i saker om overgrepsbilder av barn (§ 311), nettopp for å fremheve *personvernkrenkelsen overfor barnet på bildet.* Krenkelsen er av en annen karakter enn den som opprinnelig begrunnet straffebudet. Bestemmelsen skulle først og fremst verne den samfunnsmessige interessen i å hindre seksuelt misbruk av barn som følge av produksjon av pornografi. Men det er den individuelle *personvernkrenkelsen* som erkjennes ved vektleggingen av evighetsaspektet. Når dette fremheves enda det ikke domfelles etter et personvernstraffebud, viser det en rettsutvikling forårsaket av datautviklingen. Det har skjedd til tross for at § 311, som nevnt i kapittel 1, verken nevner datasystem eller data.

[29 Bestemmelsene er som nevnt videreført i den nye åndsverkloven, se fn. 10. Straffehjemmelen fremgår av §§ 79 og 80 i den nye loven.]

30 TAHER-2016-136649. Omtalt blant annet i *Aftenposten* 20.6.2017: «18 åring dømt for å ha delt sexbilde på Snapchat», s. 16.

[31 Se fn. 28.]

Teknologiutviklingen er årsak til tilsvarende rettslige strømninger innen EU-retten, under merkelappen «retten til å bli glemt». Google Spania mot Costeja González er den ledende avgjørelsen.[32] Saken gjaldt et varsel som lå ute på internett om tvangssalg av González' bolig i 1997 på grunn av trygdegjeld. Den opprinnelige offentliggjøringen var obligatorisk etter loven, men hendelsen lå etter hvert mange år tilbake i tid. EU-domstolen ga González medhold i at det måtte gjelde en grense for hvor lenge opplysning om tvangssalget skulle komme opp ved «googling» av navnet hans. Google ble derfor pålagt å filtrere søk på personnavn for personopplysninger lagt ut av tredjepersoner. Ytringsfriheten (informasjonsfriheten) måtte vike for personvernet. Dette er for så vidt tilsvarende synspunkt som i sin tid ble lagt til grunn i den kjente norske filmdommen i Rt. 1952 s. 1217. Visning av en spillefilm som skildret drapet på en lensmann begått på 1930-tallet, ble stanset av hensyn til personvernet til den gjenlevende drapsmannen. Hans fortid ville uunngåelig bli kjent som følge av visning, til stor skade ikke minst for familien. Han hadde sonet sin straff og etablert seg som lovlydig borger. Høyesterett mente at det grunnleggende ulovfestede personvernet i norsk rett måtte gå foran hensynet til ytringsfriheten og investeringsvernet (tapte produksjonskostnader). «Retten til å bli glemt» viderefører således eldgamle rettssetninger i en digital kontekst.

4. Ytrings- og handlingsstraffebud: Noen tolkingsspørsmål

Gjennomgangen så langt har belyst straffbare handlinger i form av ytringer. En vanlig definisjon av «ytring» er at det er tale om «formidling av et meningsinnhold fra et menneske (avsenderen) til et annet (adressaten)».[33] Når gjerningsbeskrivelsen gjelder en handling overfor et menneske *og* kan overtres ved bruk av en ytring, står vi overfor det jeg kaller et «ytringsstraffebud». I andre tilfeller er det tale om «handlingsstraffebud». Rene ytringsstraffebud, f.eks. slike som er nevnt i kapittel 3.1, kan åpenbart overtres ved informasjonsoverføring på internett. Men også bestemmelser som i utgangspunktet fremstår som handlingsstraffebud, kan la seg overtre ved bruk av ytringer. Bevisstgjøring av ytringsaspektet kan også bidra til å avklare mer spesielle tolkingsspørsmål.

4.1 «Ytringstesten» kan operasjonalisere straffebud for digitale forhold

Utgangspunktet er at dersom gjerningsbeskrivelsen lar seg oppfylle ved bruk av en ytring, kan straffebudet anvendes på internett. Spørsmålet om så er tilfellet, kaller jeg «ytringstesten». Testen er et hjelpemiddel til å kartlegge *ordlydens naturlige betydning* i relasjon til digitale forhold, fordi den bevisstgjør betydningen av om målet er en maskin eller et menneske. Dette gir en intuitiv forståelse av om og hvordan straffebudet kan overtres digitalt.

Straffebudet om ID-krenkelse (§ 202) er et egnet eksempel. Anvendelsen henger på tolking av ordet «opptrer» sammenholdt med forarbeidenes presisering av at det gjelder overfor en person.[34] Både det *å fremstå* som en annen, f.eks. ved forkledning (i den fysiske del av verden), og *å opplyse* om feil identitet omfattes. «Opptrer» omfatter derfor bruk av ytring, og

[32] EU-domstolens dom 13. mai 2014 (Sak C-131/12).
[33] Bing, op.cit., fn. 12, s. 22–23.
[34] Ot.prp. nr. 22 (2008–2009) s. 45.

bestemmelsen kan anvendes på nettet selv om det ikke fremgår uttrykkelig av ordlyden. Bestemmelsen rammer f.eks. bruk av en annens bilde på en datingtjeneste så vel som opprettelse av en webside som er forvekselbar med websiden til et kjent foretak, og publisering av innhold på en Facebook-profil som man uberettiget har tatt kontroll over. I det sistnevnte tilfellet begås ID-krenkelsen (§ 202) etter et forutgående innbrudd på Facebook-kontoen, jf. § 204 (uberettiget «tilgang til datasystem eller del av det»).

Videre kan det sluttes at bruk av et stjålet passord for å oppnå tilgang til en brukerkonto *ikke* er «å opptre» i bestemmelsens forstand, til tross for at handlingen går ut på å presentere seg som en annen. Dette er forklart i kapittel 3.2.

Jeg viser også til to andre eksempler: Bedrageri begås ved *å forlede* en annen til å foreta en handling vedkommende ikke ville foretatt, hadde hun kjent til de reelle omstendighetene. Selv om vilkåret «fremkaller, styrker eller utnytter en villfarelse» i § 371 bokstav a ikke presiserer ytringsaspektet, er tolkingen klar. Ytringstesten bidrar likevel, fordi den bevisstgjør aktuelle overtredelsesformer og dermed straffebudets anvendelighet på internett. På nettet kan det derfor tales om «ytringsbedrageri», typisk falske tilbud og betalingsløfter. Fakturasvindel på e-post er et annet betydelig problem, også dette et ytringsbedrageri.[35] Tolkingen er klar til tross for at intet i lovteksten indikerer forbrytelsens dataaspekt. Motsatt er det klart at uriktig avkryssing i NAVs elektroniske meldekort ikke er ytringsbedrageri, fordi meldekortet behandles av et datasystem.

Det siste eksemplet jeg skal nevne, er § 165 som rammer den som uhjemlet bruker «uniform eller på annen måte offentlig utgir seg for å ha offentlig myndighet». Uttrykket «utgir seg for» må tolkes på samme vis som «opptrer» i § 202, dvs. at straffebudet har en ytringsdimensjon. Forarbeidene nevner registrering av forvekselbart domenenavn.[36] Et annet eksempel kan være opprettelse av en nettside som visuelt kan forveksles med politiets offisielle portal.

Det fremgår at *formidlingsmåten* er irrelevant for subsumsjonen. Avgjørende er hvorvidt det er tale om et meningsinnhold og om adressaten er en person. Ytringsstraffebud kan derfor også overtres automatisert. Lovbryteren har f.eks. laget en mobilapplikasjon som stadig produserer falske salgstilbud. På denne måten effektiviseres gjennomføringen av bedrageriene (flere tilbud med mindre innsats). Like fullt er det lovbryteren som står bak produksjonen av uriktig informasjon og fremkaller villfarelsen hos adressatene.

Det er for øvrig innlysende at man ikke kan gå fri for ansvar under henvisning til at «det var dataprogrammet som gjorde det». I svensk rett finnes en sak som gjaldt bruk av dataprogrammet «Maggie» som deltaker i pokerspill på Svenska Spels nettsted. Tjenesten tillot ikke spillroboter, så Maggies deltakelse var ulovlig. Maggie viste seg å være en god

[35] Norsk senter for informasjonssikring (Norsis), *Trusler og trender 2016,* tilgjengelig på https://norsis.no/wp-content/uploads/2016/07/trusler-og-trender-2016_final-c.pdf.
[36] Ot.prp. nr. 8 (2007–2008) s. 334.

pokerspiller og vant over ca. 5000 spillere før hennes sanne identitet ble avslørt. Maggie ble selvsagt ikke forsøkt holdt strafferettslig ansvarlig.[37] Bedømt etter norsk rett måtte handlingen anses som et ytringsbedrageri, utført ved uriktig å bekrefte å være en person. Det forledet motspillerne til å delta på premisser de ikke kjente (mot en datamaskin).

Nå som kunstig intelligens på nytt har fått vind i seilene, kan man gjøre seg ytterligere noen tanker om den rettslige betydningen av bruk av tale. Følgende anekdote fortalt av professor i informatikk Jan Arne Telle er illustrerende:[38] Episoden utspant seg ved middagsbordet sammen med hans sønn. Plutselig sa sønnen til sin iPhone som lå på bordet: «'Hey Siri, send my sister a message saying I will be ten minutes late' […]. En kvinnestemme svarte: 'Who is your sister', så han la til: 'It is Aurora.'» Faren reagerte med forbløffelse over at sønnen fikk gjort det han ville uten engang å legge fra seg kniv og gaffel, og uten å involvere noen andre. «I alle dager, hva blir det neste, tenkte jeg.»[39]

E-posten var selvsagt en ytring fra sønnen til søsteren. Talen til iPhonen, derimot, var en handling rettet mot datamaskinen. Endepunktet var ikke et menneske og kommandoen ikke en ytring. Til sammenligning er kommandoen «Sitt!» til en hund heller ikke en ytring. [Hvis teknologien ikke setter begrensninger på den digitale assistentens funksjonalitet, kan eksempelvis et regulært skadeverk utføres på et annet datasystem, rent talestyrt, bare ved å fortelle den digitale assistenten på ens egen datamaskin hva som ønskes utført. Den digitale assistenten er et redskap, sml. en hund, som kan tenkes å inngå i utførelsen av så vel handlings- som ytringsforbrytelser.[40]]

Hvordan stiller det seg da med følgende eksempel: Jeg har lånt Heidis iPhone for å ringe hjem. Jeg benytter anledningen til å si til iPhonen: «Hei, jeg er Heidi, betal 500 kroner til Inger Marie med Vipps». Dermed har jeg brukt Heidis identitet for å overføre penger til meg selv. Er dette datainnbrudd, underslag, bedrageri, databedrageri, identitetskrenkelse eller ingen av delene så det er behov for et nytt straffebud for å fange opp handlemåten? Burde gjerningsbeskrivelsen tydeligere enn i dag uttrykke hvorvidt handlingen gjelder direkte overfor et annet menneske eller ei, og burde ytringsaspektet tydeligere innarbeides i straffebud som er aktuelle for menneskelig interaksjon på internett?

4.2 Ytring og handling vs. informasjon og data

Når man befatter seg med strafferett, er det lett å forestille seg konkrete handlinger som slag, spark, fysisk tvang, innbrudd og ødeleggelse. I digital kontekst er det imidlertid nødvendig først å ha et forhold til størrelsene «informasjon» og «data», som følger skillet mellom ytring og handling. «Informasjon» tar sikte på meningsbærende innhold, mens «data» er et digitalt

[37] Södertörns tingsrätts dom 2014-12-19 i mål nr. B 5929-13, overprøvd i Svea hovrätts dom 2016-02-18 i mål nr. B 680-15. Se omtale i Jonas Ekfeldt, *Om informationstekniskt bevis,* PhD.-avhandling, Juridiska institutionen, Stockholms universitet 2016, s. 164.
[38] Jan Arne Telle "Den nye maskinlæringen: Kunstig intelligens eller bare gode verktøy? ", *Nytt Norsk Tidsskrift* 02/2017, s. 192-204, på s. 192.
[39] Ibid.
[[40] Teksten i klammeparentes er tilføyd i opptrykket for å klargjøre anekdotens rettslige relevans.]

objekt på linje med et fysisk objekt. Det gir en enkel taksonomi for å beskrive grunnleggende trekk i det digitale landskapet. Visse konkrete handlinger som nevnt kan begås digitalt, f.eks. ødeleggelse av data. Men også informasjon er en relevant størrelse. Da handler det om straffbare handlinger på meningsplanet mennesker imellom.

Den språklige variasjonen i datakrimstraffebudene uttrykker imidlertid en annen uklar tilnærmingsmåte: Således bruker § 201 uttrykket «databasert informasjon»; § 205 bokstav b (ulovlig avlytting/overvåking) «informasjon som overføres ved elektroniske […] hjelpemidler»; § 206 (driftshindring) «informasjon [i] et datasystem»; § 371 bokstav b (databedrageri) «uriktig eller ufullstendig opplysning, endrer data eller datasystem […] eller på annen måte påvirker resultatet av en automatisert databehandling». Som nærmest for «å toppe» det hele benyttes uttrykket «informasjonsbærer» i § 361 annet ledd (det strafferettslige dokumentbegrepet). «Informasjonsbærer» er definert i § 76 som nevner «trykt skrift eller annet som formidler en skriftlig, auditiv eller elektronisk lagret informasjon».

I kontrast til dette beskriver § 351 annet ledd kort og godt skadeverk mot «andres data». Bestemmelsen føyer seg til den tradisjonelle skadeverksbestemmelsen i første ledd, om skade på «en gjenstand som tilhører en annen». Annet ledd lyder slik:

> «For skadeverk straffes også den som uberettiget endrer, gjør tilføyelser til, ødelegger, sletter eller skjuler andres data.»[41]

Straffebudet om befatningsforbud for tilgangskoder/passord og hackerutstyr (§ 201) er tungt tilgjengelig, men bruk av den innledende taksonomien letter tolkingen. De straffbare handlemåtene er *fremstilling, anskaffelse, besittelse og tilgjengeliggjøring.* Praktisk sett kan tilgangskoder (passord) gjettes, mottas nedskrevet på en lapp, bli opplyst muntlig eller på e-post, ligge integrert i kodebrikker og adgangskort, i krypterte datafiler osv. Hackerutstyr kan foreligge som dataprogram (kilde- eller objektkode) og fysiske innretninger. Befatningen kan således gjelde informasjon, data og fysisk utstyr. Det er unødvendig å gå via moralske betraktninger om betenkelighetene ved «sinnelagsstrafferett» for å innse at det ikke er straffbart *å gjette eller erindre* en annens passord (det ses bort fra maskinelle former for passordknekking). *Anskaffelse* og *besittelse* må åpenbart tolkes innskrenkende når det er tale om *informasjon*. Derimot er det intet i veien for å straffe forsettlig spredning av passord, også om det skjer muntlig. Mens mottakeren vanskelig kan straffes for tilfeldig *å ha hørt det*, er det anskaffelse dersom dette var planlagt. Videre er det enkelt å forstå at alle alternativene er anvendelige på data som digitalt objekt, på samme vis som om det var tale om et fysisk objekt. Straffebudet er altså både et ytrings- og et handlingsstraffebud. Befatningsforbudene i § 311 (overgrepsbilder) og § 370 (utstyr for dokumentfalsk) er av tilsvarende karakter.

Videre kan man stusse over formuleringen «informasjon [i] et datasystem» i § 206 (driftshindring). Bestemmelsen slår ned på digitale handlinger som utsetter datasystemet for fare for å bli satt ut av funksjon. Det er tale om *bruk av data som middel* til å oppnå den

[41] Jeg har redegjort for bestemmelsen i *Datakriminalitet,* Fagbokforlaget, Bergen 2016, kapittel 6.

skadelige virkningen. Det kreves ikke stor datakompetanse for å forstå at straffebudet ikke kan overtres ved bruk av en ytring. Ordet «informasjon» er derfor egnet til å forvirre.

Datakrimstraffebudene har særlig vært begrunnet i behovet for å styrke påliteligheten og tilliten til data og datasystemer.[42] Man kunne derfor heller tale om «data*sikkerhets*kriminalitet». Datasystemer er strafferettslig å regne som en gjenstand og beskyttet etter de vanlige reglene om dette. Det er derfor *dataenes* sårbarhet som er hovedbegrunnelsen for datakrimstraffebudene. Bestemmelsene beskytter mot uberettiget endring/sletting og mot at uberettigete personer skaffer seg innsyn og eventuelt kommer i posisjon til å foreta skadevoldende handlinger mot data. Det synes derfor som begrepet «data» kunne være dekkende *i alle de nevnte bestemmelsene.* Bruk av ordet «informasjon» er uheldig når det likevel ikke er tale om ytringer.

Ytterligere forenkling kan oppnås ved å bruke § 351 annet ledd (med noen justeringer) som *grunndelikt for bestemmelsene om* datasikkerhetskriminalitet*.* Gjerningsbeskrivelsen beskriver vanlig modus for å ramme data og (indirekte) datasystemer. Det er *variasjon i motiv* som i realiteten skiller handlingene fra hverandre: Dersom handlingen begås med uberettiget vinnings forsett, foreligger databedrageri, jf. § 371 bokstav b. Dersom den begås for å hindre driften av et datasystem, er det tale om driftshindring, jf. § 206. Dersom den begås for å overta kontrollen over et datasystem ved å innplassere skadevare, f.eks. en overvåkingstrojaner, kan det være tale om datainnbrudd, jf. § 204, og ulovlig overvåking, jf. § 205 bokstav b. Dersom den begås for å skade et datasystem, er det et regulært skadeverk mot en «gjenstand», og da er man over i § 351 første ledd.

Poenget er at *manipulasjon av data er selve kjernen i handlemåten for mange dataforbrytelser.* Loven ville gjort dette klarere ved å konsentrere beskrivelsen ett sted. Mylderet av alternativer tjener mer til å forvirre enn å skape forståelse. Språklig ensartethet ville gitt større klarhet og dermed vært i bedre samsvar med legalitetsprinsippet.

Som et siste poeng synliggjør sondringen mellom ytring og handling et problem vedrørende *forsettets omfang* i bedrageritilfeller på internett. For *ytringsbedrageri* innebærer forsettet at lovbryteren må være klar over at hun forleder en person, mens for *databedrageri* at hun påvirker resultatet av en automatisert databehandling. Lovens forutsetning om at lovbryteren vet hva slags adressat hun står overfor, slår ikke nødvendigvis til på internett. Hun blir presentert for en webside eller en applikasjon og gjør det som skal til for å oppnå ytelsen. Hun behøver ikke ha skjenket en tanke til om den andre enden er en datamaskin eller en kundebehandler. [Og paradoksalt nok kan et samtaleprogram (chatbot) skape en feilaktig oppfatning om å ha med et menneske å gjøre.[43]] Bedrageribestemmelsene er altså ikke helt treffende for nettverksbaserte transaksjoner, og kunne behøve revisjon.

[42] Se bl.a. Ot.prp. nr. 22 (2008–2009) s. 62; NOU 2007: 2 (Datakrimutvalget II) s. 81 og 154.
[43] Tilføyd i opptrykket.]

5. Tingenes internett: Legemskrenkelser og skadeverk

«Tingenes internett» betyr som nevnt at nettverksteknologien inkluderer individer og objekter som vi tidligere ikke har tenkt på som del av datasystem/-nettverk. Dette muliggjør både drap, legemskrenkelse og skadeverk. Vi kan nå vende tilbake til eksemplene i kapittel 1: (i) Manipulasjon av blodsukkermåler/pacemaker kan innebære kroppskrenkelse eller drap, jf. § 271 eller § 275. (ii) Hundemishandlingen er straffbar etter dyrevelferdsloven § 14 bokstav a, jf. § 37.[44] (iv-vi) Utkoblingen av den elektroniske dørlåsen, tuklingen med Teslaen, og det trafikale signalsystemet er grovt skadeverk og sabotasje, jf. § 352 og § 192.

Hva så med arvetanten (iii)? Her følges resonnementet i punkt 4.1. Hun feildoserte fordi nevøen manipulerte programmet som fortalte når medisin skulle tas. Programmet formidler ytringer, siden instruksene ellers ville vært gitt av en person (helsearbeider). Nevøens endringer i programmet innebærer at det er *hans ytringer* som forårsaker overdoseringen og dermed dødsfallet (som var motivet). Etter § 275 er det imidlertid likegyldig om drapet skjer ved en ytring eller en handling, jf. «dreper en annen». Digitaliseringen innebærer dermed ikke en vesensforskjellig endring sammenlignet med tradisjonelle (fysiske) overtredelsesmåter.

6. Rettspolitisk vurdering

Jeg mener å ha vist at det er betimelig å stille spørsmål ved om det er viktig å straffe for handlingens dataaspekt når de tradisjonelle bestemmelsene åpenbart er anvendelige? I henhold til reglene om konkurrens skal det nemlig straffes for datasikkerhetskrenkelsen i tillegg til den tradisjonelle bestemmelsen. For ytringsforbrytelsene oppstår likevel ikke spørsmålet, fordi de utføres ved ordinær bruk av tjenestene, om enn for ulovlige formål.

På begynnelsen av 2000-tallet fremsto det som viktig spesifikt å ramme krenkelser mot data og datasystemer. Men den gang visste man ikke hvor omfattende teknologiutviklingen kom til å bli. Når teknologien er integrert så å si overalt, burde lovgivningen vurderes på nytt. Det er et poeng i seg selv å gjøre straffeloven så enkel og tilgjengelig som mulig siden det har stor betydning for kunnskapen om hva som er straffbart. Av hensyn til effektiviteten i straffesaksbehandlingen bør det også unngås å pålegge politiet etterforskingsoppgaver knyttet til kompliserte datasikkerhetstema i et stort antall saker.

Jeg ser for meg at to grep kunne være hensiktsmessige *de lege ferenda.* Det ene er å innføre bruk av datateknologi blant de skjerpende omstendighetene som er regnet opp i § 77, eventuelt presisere at det omfattes av bokstav a om lovbrudd som er begått med «midler eller metoder som er særlig farlige eller har stort skadepotensial». Siden det normalt ikke kreves at disse omstendighetene omfattes av forsettet, kunne dette lede til forenkling av etterforskingstemaet. I stedet for å anvende datakrimstraffebud i konkurrens med en tradisjonell bestemmelse kunne den tradisjonelle bestemmelsen anvendes med skjerpelse

[44] Lov om dyrevelferd av 19. juni 2009 nr. 97. Voldsbegrepet i § 14 omfatter unødig påføring av angst, stress eller andre mentale påkjenninger som gir redusert velferd; Ot.prp. nr. 15 (2008–2009) s. 103.

etter § 77. Dette burde imidlertid også gjelde for straffbare ytringer på internett på grunn av den store og vedvarende spredningen.

Det andre grepet er uavhengig av det første. Det er utvilsomt behov for å kunne straffe alvorlige angrep på data og datasystemer, siden den digitale sårbarheten øker i takt med den digitale avhengigheten. Loven kunne imidlertid foretatt en tydeligere differensiering enn i dag. Det gir f.eks. liten mening at innbrudd på serveren til en høyteknologibedrift og innbrudd på en Facebook-profil straffes etter samme bestemmelse med 2 års strafferamme (§ 204). Det er også underlig at programmerere av skadevare og andre tilretteleggere for datasikkerhetskriminalitet bare risikerer fengsel inntil 1 år, jf. § 201. Ifølge Europol er disse de største truslene mot et rimelig lovlydig digitalt samfunn og bør gis topp prioritet i strafforfølgningen.[45] Straffeloven kommuniserer imidlertid ikke dette.

Uklare begreper, lav strafferamme, lav oppdagelsesevne og anmeldelseshyppighet – alt dette bidrar til at datakrimbestemmelsene blir lite brukt. Politiet må nok kunne etterforske datatekniske tema og utnytte databevis, men ikke alle kan ha avansert kompetanse. Effektivitet i strafferettspleien er et viktig formål for stadige reformtiltak i politiet, og loven bør bidra med å gi tydeligere signal enn i dag om hva som bør prioriteres.

[45] Europol, *Internet Organised Crime Threat Assessment (iOCTA) 2016,* s. 15. [Dette rådet gjelder fortsatt, jf. *iOcta 2018*, s. 29.]