Sorenskriver Stein Schjølberg (Mai 2007):

Høringsuttalelse til NOU 2007:2 – Lovtiltak mot datakriminalitet – Delutredning II

Det vises til brev av 03.03.2007 med anmodning om høringsuttalelse.

Undertegnede var leder av datakrimutvalget som avga Delutredning I, og har fungert som ekspert for internasjonale organisasjoner om den globale harmonisering av lovtiltak mot cybercrime. Jeg deltar i den internasjonale informasjonsutveksling om cybercrime som foredragsholder og viser for øvrig til min web side: www.cybercrimelaw.net.

Artikkelen "Terrorism in Cyberspace – Myth or reality?" (mai 2007) vedlegges. En artikkel om "Phishing-international and national criminal law" og "Global harmonization of cybercrime legislation" vil ble ettersendt i løpet av sommer/høst 2007.

Høringsuttalelsen inneholder i Del I, generelle merknader om den internasjonale og nasjonale utvikling, plassering av straffebud i straffeloven eller særlovgivningen, behovet for eget kapittel for straffbare handlinger rettet mot informasjon og informasjonsutveksling, enkelte merknader til rettsstridsreservasjonen og forberedelseshandlinger, merknader til grunnleggende begreper og til skyldkravet.

Merknader til lovutkastet fra datakrimutvalget II i NOU 2007:2 behandles i II. Henvisninger til fremmed rett og det internasjonale samarbeidet behandles i III. Merknader til det lovutkast som høringsuttalelsen vil inneholde behandles i IV. Høringsuttalelsens lovutkast behandles i V.

Lovutkast som angår særlovgivningen vil ikke bli behandlet i større utstrekning enn merknader til lovutkastet i NOU 2007:2.

I. Alminnelige merknader

1. Det er i Delutredning I om lovtiltak mot datakriminalitet (NOU 2003:27) redegjort for den nasjonale og internasjonale utvikling frem til utredningen ble avgitt 4.november 2003. Etter denne tid har utviklingen av informasjons- og kommunikasjonsteknologien fortsatt å gå svært raskt. Sett i historisk sammenheng kan den teknologiske revolusjonen som nå foregår sammenlignes med den industrielle revolusjon på 1800-tallet. Fra 2000 til mars 2007 har bruken av Internett årlig økt med 208 % i

gjennomsnitt og det antas at 1,14 milliarder mennesker bruker Internett av en samlet befolkning på jorden på ca 6,6 milliarder.

Kriminaliteten flytter også over på Internett og gjennomføres ved bruk av, eller retter seg mot datasystemer og nettverk som cyberspace er bygget på. Nye former for kriminalitet har oppstått og nye globale betegnelser som for eksempel botnet, phishing, pharming er oppstått. I denne utviklingen må lov og orden også sikres og utvikles i cyberspace som i det globale samfunn for øvrig. Utviklingen har også vist at den organiserte kriminaliteten i stadig større utstrekning utvikler nye metoder for å gjennomføre straffbare handlinger eller til å angripe datasystemer og nettverk. Utviklingen har likeledes ført til en økende uro for at terrorister skal rette sine angrep mot datasystemer og nettverk som er av vital betydning for statenes infrastruktur. Dommen i Københavns byrett av 11.04.2007 og de kordinerte angrep på statlig og privat informasjons infrastruktur i Estland i mai 2007 er eksempler på at dette kan bli en realitet.

Det er på samme måten nødvendig å vurdere behov for nye bestemmelser og virkemidler i straffeprosessloven. I en global etterforskning og straffeforfølgning må de enkelte lands prosessbestemmelser også være tilpasset hverandre. Tvangsmidlene må tilpasses utviklingen i cyberspace, og må være felles for alle straffbare handlinger.

Innføringen av nye bestemmelser i straffe- og straffeprosesslovgivningen krever at borgerne sikres en adekvat beskyttelse av menneskerettigheter og personvern. De lovtiltak som gjennomføres må derfor være underlagt nasjonale og internasjonale rettssikkerhetsprinsipper i henhold til de globale konvensjoner.

2. Utviklingslinjer i Norge

Som kjent ble det gjennomført endringer i straffeloven og straffeprosessloven i forbindelse med tilpasningen til Europarådets konvensjon om cybercrime idet Stortinget vedtok å endre straffeloven §§ 12 1.ledd nr 3 bokstav a og 145, samt vedtok ny bestemmelse i § 145 b. I straffeprosessloven ble det gitt ny bestemmelse i § 199 a og § 215 a.

3. Internasjonale utviklingslinjer

Europarådets konvensjon om cybercrime trådte i kraft 01.07.2004 og konvensjonen er ratifisert av 19 stater i tillegg til at 24 stater har undertegnet konvensjonen uten ratifikasjon (mai 2007). Mexico og Costa Rica har søkt om tilslutning og er invitert til dette av Europarådet. Europarådet har i tillegg vedtatt en annen konvensjon "Council of Europe Convention on the Prevention of Terrorism" i 2005 og denne konvensjonen trer i kraft 01.06.2007.

På grunnlag av Europarådets konvensjon om cybercrime skapes nå forutsetninger for en global rettshåndhevelse basert på felles prinsipper for straffbarhet og straffeforfølgning. Ved å ratifisere eller slutte seg til konvensjonen, eller implementere de standarder og prinsipper som den inneholder, forsikrer statene seg at de nasjonale bestemmelser omfatter cybercrime. Den harmonisering av nasjonale straffe- og straffeprosessuelle bestemmelser som nå foregår reduserer mulighetene for "Datahavens", stater med jurisdiksjon hvor cybercrime helt eller delvis er straffefritt. I en global etterforskning og straffeforfølgning må de enkelte lands prosessbestemmelser også være tilpasset hverandre. Et effektivt internasjonalt samarbeid er avgjørende i etterforskningen av den globale cybercrime og sikring av elektroniske bevis i slike saker.

EU vedtok sin Rådsrammebeslutning (Council Framework Decision) i 2005. Rådsrammebeslutningen er et supplement til Europarådets konvensjon om cybercrime og inneholder bestemmelser om uberettiget tilgang til informasjonssystemer, uberettiget forstyrrelse av data og datasystemer. Særlig skal også nevnes artikkel 10 som inneholder prinsippet om "Prosecute or Extradite".

Av FN organisasjonen er det International Telecommunication Union (ITU) i Geneve som har vært den mest aktive med å fremme en global harmonisering av straffelovgivningen om cybercrime. ITU holder årlige møter om blant annet dette spørsmål, senest i mai 2007. Basert på Europarådets konvensjon om cybercrime og anbefalinger fra FN organisasjoner, EU, G8-statene, Organisasjonen for Amerikanske stater (OAS), Asian Pacific Economic Cooperation (APEC), Det Britiske samveldet, Association of Southeast Asian Nations (ASEAN) og OECD foregår for tiden en

global harmonisering av nasjonale straffe og straffeprosessuelle bestemmelser som angår cybercrime.

I tillegg skal nevnes at riksadvokater fra 30 stater avholdt møte i Oslo i september 2006 for å drøfte kampen mot terrorisme, se den vedlagte artikkel side 1 og 5. I tillegg er Interpol aktive og har avholdt en global konferanse i Egypt i 2005 og skal avholde neste konferanse i India i september 2007.

Det konsultative råd for europeiske dommere (CCJD) vedtok i 2006 en rekke prinsipper som angikk terrorisme, men som får tilsvarende anvendelse når staters informasjons infrastruktur er målet, se den vedlagte artikkel side 7–8. Det er reist spørsmål om slike saker allerede i dag kan etterforskes og avgjøres av den internasjonale straffedomstolen i Haag, se vedlagt artikkel side 10.

4. Plassering av straffebud i straffeloven eller særlovgivningen

Vår tradisjon tilsier at straffebud om alvorlige forhold samles i en egen straffelov, mens forhold av mindre alvorlig og spesiell karakter reguleres av særlovgivningen. Lovtiltak om datakriminalitet omfatter alvorlige forhold og bør plasseres i straffeloven. Unntak bør skje hvor det gjelder mer tekniske spørsmål som for eksempel definisjoner av data, datasystemer og lignende samt andre forhold av mer teknologisk karakter hvor det er naturlig at de plasseres i det regelverk i særlovgivningen som regulerer teknologiske spørsmål, for eksempel e-kom loven. Bestemmelsene i straffeloven bør være mest mulig teknologisk nøytrale av hensyn til den teknologiske utviklingen. Handlingsnormer som teknologisk sett saklig hører sammen bør behandles i samme lov. Det gir større oversikt og brukervennelighet og man kan lettere benytte seg av et forskriftsverk som understøtter spørsmål av teknologisk karakter. En rask teknologisk utvikling kan lettere la seg tilpasse ved å benytte særlovgivningen med forskriftsverk. Hensynet til teknologisk oversiktlighet og saklig sammenheng bør være avgjørende for plassering av straffebud i særlovgivningen.

5. Eget kapittel for vern av data, informasjon og informasjonsutveksling

Det foreslås at Straffelovkommisjonens forslag til ny straffelov kapittel 23 deles i a og b. Straffelovens kapittel 23 a inneholder de alminnelige lovbestemmelser til vern av data, informasjon og informasjonsutveksling. Kapittel 23 b bør inneholde spesialbestemmelser om brudd på taushetsplikt, brudd på bedriftshemmelighet m.v.

Særskilte straffebestemmelser for datakriminalitet skaper en større forebyggende og moralskapende virkning enn tvilsomme tolkninger av eksisterende straffebestemmelser. Gjerningsmannen vil da bli dømt etter disse særlige bestemmelsene, og ikke etter straffebestemmelser som bare omfatter tilfeldige eller ubetydelige sider ved handlingen. Hensynet til våre internasjonale forpliktelser tilsier klare og utvetydige straffebestemmelser som tilkjennegir at alle former for cybercrime straffes i Norge.

For å kunne etablere etiske standarder i cyberspace, må også straffebestemmelsene bli utformet så klare, entydige og presise som mulig. Særskilte straffebestemmelser om datakriminalitet vil også forenkle bevisføringen for påtalemyndighet og forsvarer, og rettspraksis vil lettere kunne bidra med å etablere klare rettsavgjørelser og skape viktige presedenser av betydning for informasjons- og kommunikasjonsteknologien. Det er naturlig å betrakte datakriminalitet som et eget spesialområde, som bør få en mest mulig samlet regulering ved et eget kapittel i straffeloven. Lovtekniske hensyn kan allikevel føre til at de eksisterende straffebestemmelser naturlig bør benyttes, for eksempel ved bedrageri og dokumentfalsk. Den forenkling man oppnår, slik som den nåværende straffelov § 270 nr 2 bør vedvare i den nye straffelov.

6. Rettsstridsreservasjonen

Straffebestemmelsene i den nåværende straffelov inneholder et krav om at handlingen må være rettsstridig eller uberettiget. Disse begreper inneholder den generelle reservasjon om at det ikke er meningen å ramme alle de handlinger som ellers går inn under straffebestemmelsen. De vanlige straffefrihetsgrunner som samtykke, nødrett og nødverge får anvendelse. Handlingen kan også være berettiget fordi den har hjemmel i lov, avtale eller annet rettsgrunnlag. Handlingen kan også være lovlig foretatt av

offentlig myndighet, forvaltningsmyndighet i stat eller kommune eller politi. Lovlige handlinger og aktiviteter som er en del av utviklingen, design, drift og vedlikehold av datasystemer og nettverk omfattes ikke av bestemmelsen. Hvis ansatte handler i strid med instrukser vil handlingen normalt være straffbar. Tilgangen til datasystemer kan være berettiget for eksempel hvis den sikkerhetsansvarlige har fullmakt til å forsøke å forsere en passordbeskyttelse for å teste systemsikkerheten. Slik testing med samtykke av den berettigede medfører ikke straffeansvar.

Eksemplene viser nødvendigheten av særlig i informasjons- og kommunikasjonsteknologi og ha en rettsstridsreservasjon fordi det ikke er meningen å ramme alle de handlinger som ellers ville gå inn under gjerningsbeskrivelsen i straffebestemmelsen. Det er særlig viktig i informasjons- og kommunikasjonsteknologien utvetydig å ha en reservasjon i selve straffebestemmelsen. At en rettsstridsreservasjon finnes i straffebestemmelsen er likeledes bedre i overensstemmelse med våre internasjonale forpliktelser i henhold til Europarådets cybercrime konvensjon, hvor alle artikler som angår straffebestemmelser inneholder begrepet ”Without right”.

7. Forberedelseshandlinger

Det har vært en lovgivningspolitisk tradisjon ikke å gjøre forberedelseshandlinger straffbare. Men i de senere år har det vært nødvendig å gjøre unntak i flere forhold, senest lovforslag om forebygging av terrorvirksomhet.

Innføringen av informasjons – og kommunikasjonsteknologien har medført at enkelte handlinger som ville være forberedelser ble gjort straffbare, se for eksempel straffelovens § 145 b. Denne bestemmelse bør for øvrig i forbindelse med vedtakelse av ny straffelov utvides til og også omfatte de øvrige forberedelseshandlinger som er nevnt i Europarådets konvensjon om cybercrime artikkel 6. Endringen bør være i overensstemmelse med justisdepartementets forslag i Ot.prp. nr 40 (2004-2005). Dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer (hackerverktøy) bør medtas i bestemmelsen. Lovforslaget var ment å omfatte alle befatningsformer som er omhandlet i konvensjonens artikkel 6. Justiskomiteen sluttet seg ikke til forslaget fra

justisdepartementet. Flertallets begrunnelse i justiskomiteen var et ønske om ikke å kriminalisere slike handlinger. Dette innebærer, som også påpekt av mindretallet, at det ikke er straffbart i dag å gjøre datavirus og hackerverktøy tilgjengelig for andre på et nettsted, selv om en med sikkerhet kan si at de vil bli brukt til å begå andre former for cybercrime av andre gjerningsmenn.

Særlig i informasjons- og kommunikasjonsteknologien forekommer en rekke forhold som kan begrunne et selvstendig straffebud for forberedelseshandlinger. I tillegg til datavirus og hacker verktøy, har utviklingen ført til introduksjon av spam, botnet, phishing, pharming og lignende. Behovet for å straffesanksjonere besittelse og disposisjoner av slike er tilstede.

Både svensk og dansk rett har bestemmelser som rammer forberedelseshandlinger. Den danske straffelov § 21 rammer "handlinger som sikter til å fremme eller bevirke utførelsen av en forbrytelse". Bestemmelsen ble senest brukt i den foran nevnte dom i København byrett av 11.april 2007. Svensk rett ble endret den 1.juli 2001 ved at bestemmelsen om forberedelse til brott ble endret til å omfatte "befattning med något som er særskilt egnat att anvendas som hjelpmedel vid ett brott". Endringen tok sikte på å modifisere straffeansvaret slik at det ikke bare omfattet befatning med fysiske gjenstander, men også at befatning med immaterielle objekter kunne være straffbar som en forberedelse. Som eksempel ble det i motivene for lovendringen særskilt vist til datavirus og annen programvare som er fremstilt utelukkende med det formål å foreta uberettiget tilgang til data eller annen datakriminalitet.

Høringsuttalelsen foreslår i sitt lovutkast også i Norge en særskilt bestemmelse som gjør forberedelseshandlinger med data og datasystemer straffbare som selvstendige forbrytelser.

8. Grunnleggende begreper i informasjons- og kommunikasjonsteknologien

Det har også vært en tradisjon i norsk strafferett og gjøre gjerningsbeskrivelsen i straffebudene mest mulig teknologisk nøytrale. Informasjons– og kommunikasjonsteknologien utvikler seg med voldsom fart.

Data er magnetiske impulser og en elektronisk representasjon av informasjon. Informasjonen i seg selv kan ikke lagres eller overføres. Informasjon oppstår først i et menneskes bevissthet når data blir sett, hørt, følt eller på annen måte brakt innenfor rekkevidden av sanseapparatet, se Knut S. Selmer, (Lov og rett 1995 side 149-150).

Det er en sikker oppfatning i norsk rettspraksis og teori at data ikke er en gjenstand. Lagringsmedia kan være gjenstander men ikke data i seg selv. Stortinget har utvetydig klargjort dette i sitt vedtak til en ny straffelov første del, og har i sine merknader til legaldefinisjonen av gjenstand uttalt: ”Informasjon i datasystemer med videre skal fortsatt ikke regnes som gjenstand”. Det er i Delutredning I redegjort for de grunnleggende begreper i informasjonsteknologien når det gjelder data, datasystemer, tjenestetilbyder og trafikkdata, og det vises til disse.

Begrepet tyveri er i norsk strafferett definert i straffeloven § 257 og forutsetter at en gjenstand borttas. Når data ikke er gjenstand kan ikke definisjonen av tyveri anvendes. Etter alminnelig forståelse må en gjenstand være av fysisk beskaffenhet, og immaterielle objekter faller utenfor begrepet. Som nevnt er lagrede data bare magnetiske impulser og den informasjonen dataene representerer har klar immateriell karakter. Betegnelsen tyveri bør således ikke benyttes ved disposisjoner over data eller datasystemer, bortsett fra hvor det foreligger tilknytning til et lagringsmedium.

9. Skyldkravet

Den nye straffelov har i §§ 21-23 bestemmelser om skyldkrav. Hovedregelen er at det er bare de forsettlige handlinger som rammes, jf strl. § 21. Bestemmelsene om vern av data, informasjon og informasjonsutveksling må følge de alminnelig prinsipper som er nedfelt i disse bestemmelser.

II. Merknader til lovutkastet i NOU 2007: 2 - Lovtiltak mot datakriminalitet

1.

Overskriften til kapittel X inneholder uttrykket "databasert" informasjon. Dette er ikke et vanlig uttrykk når overskriften ellers inneholder både data og informasjon. Uttrykket datasystemer er benyttet, og det forutsettes at dette er det samsvar med Europarådets konvensjon om cybercrime. Når flere datasystemer knyttes sammen i et nettverk brukes allikevel betegnelsen datasystemer.

§ 1 - Definisjoner

Det er ingen tradisjon for at definisjoner av ord og uttrykk omtales i straffeloven i større utstrekning enn de som nevnes i det nye straffelovs kapittel 2 om legaldefinisjoner. Det må reises spørsmål om definisjonene i lovutkastet § 1 naturlig hører hjemme i straffeloven. Hvis det i det hele tatt er ønskelig med slike definisjoner har de mer saklig sammenheng med definisjonene i lov om elektronisk kommunikasjon av 04.07.2003 nr 83. Særlig gjelder dette definisjonen i § 1 litra e. Det foreslås således at definisjoner ikke omtales i nytt kapittel om datakriminalitet.

§ 2 - Elektronisk kartlegging av datasystem

En bestemmelse om elektronisk kartlegging av datasystem har nær sammenheng med lov om elektronisk kommunikasjon av 04.07.2003 nr 83 og bør eventuelt inntas i denne lov. I den raske teknologiske utviklingen bør hensynene til teknologisk oversiktlighet og saklig sammenheng tilsi en plassering i særlovgivningen, hvor det gis adgang til hensiktsmessig bruk av et forskriftsverk.

§ 3 – Ulovlig anbringelse av utstyr m.v

Visse forberedelseshandlinger til andre bestemmelser i kapittelet er her gjort straffbart som selvstendig forbrytelse. Det må reises spørsmål om hvorfor utkastet begrenser straffbarheten til utkastene §§ 5og 6 samt § 10. Utviklingen av informasjons- og

kommunikasjonsteknologien bør føre til at forberedelseshandlinger til alle straffebestemmelser i kapitlet om datakriminalitet gjøres straffbart, se høringsuttalelsens lovutkast.

§ 4- Ulovlig tilgang til datasystem

Den nåværende straffelov § 145 annet ledd har fungert rimelig tilfredsstillende og bør videreføres med enkelte endringer. Det må likeledes reises spørsmål om redigering av § 4 første ledd som inneholder to rettsstridsreservasjoner. En tekst bør antydningsvis lyde som følger:

" Den som uberettiget skaffer seg tilgang til data som er lagret i et datasystem, straffes med bøter eller fengsel inntil 3 år".

Tidligere utredninger har ikke funnet grunn til å etablere særskilt straff for lite datalovbrudd. Europarådets konvensjon om cybercrime åpner for å gjøre mindre eller ubetydelige lovbrudd straffefri. Dette bør Norge fortsatt legge til grunn.

§5- Informasjonstyveri og § 6- datatyveri

Det må reises spørsmål om behov for å skille mellom disse to former. Under enhver omstendighet er betegnelsen "tyveri" utilfredsstillende, og det vises til bemerkningene foran og henvisningene til den nye straffelovs legaldefinisjoner og bemerkningene i justiskomiteen.

Det er den uberettigede tilgang og innsyn i data i seg selv som skal gjøres straffbar. Det er tilstrekkelig at gjerningsmannen bare observerer og leser informasjonen i datasystemet, selv om han ikke tilegner seg kunnskapene eller forstår innholdet i informasjonen.

Det må reises spørsmål om ikke utkastet §§ 4-6 kan samles i en straffebestemmelse. Når det gjelder bruken av uttrykket "databasert informasjon" vises til bemerkningene foran.

§ 7- Datamodifikasjon

Å benytte seg av uttrykket ”modifikasjon” i norsk sammenheng har et noe gammelmodig preg. Den som uberettiget endrer, ødelegger, sletter eller skjuler andres data er i Europarådets konvensjon om cybercrime betegnet som ”data interference”. Straffelovkommisjonen foreslår også at det inntas en bestemmelse som gir et strafferettslig vern mot uberettiget endring, sletting eller tilføyelse av informasjon som er lagret ved elektroniske midler. Om handlingen betegnes som dataskadeverk, dataforstyrrelse og lignende kan være en smakssak. Handlingene må likeledes avgrenses mot elektronisk dokumentfalsk hvor resultatet i hovedsak er logisk lesbart.

§ 8- Uberettiget bruk av datasystem m.v

Slik bestemmelse er tidligere foreslått så langt tilbake som 1985, men ved lovendringene i 1987 fikk straffeloven ny § 261 som ser den uberettigede bruk i en større sammenheng som bruk eller forføyning over en løsøregjenstand som inkluderte datamaskiner. I engelsktalende land ble handlingen betegnet som ” theft of services”. Det var den ulovlige bruk av datamaskiner som ble gjort straffbar, sammen med andre former for uberettiget bruk eller forføyning over annens mann løsøregjenstand. Straffelovens § 261 straffer således ulovlig bruk av datautstyr.

Det er et lovgivningspolitisk spørsmål om man skal skille ut ulovlig bruk av datasystemer i en egen straffebestemmelse eller opprettholde den samme løsning man valgte i 1987.

Når det gjelder uberettiget bruk av elektroniske kommunikasjonsnett antas at dette mer naturlig har sin saklige sammenheng med bestemmelsene i lov om elektronisk kommunikasjon. Det samme gjelder § 8 første ledd annet punktum om bruk av andres tilgangspunkt til Internett i usikret trådløst elektronisk kommunikasjonsnett. Under enhver omstendighet antas at uttrykket ”Internett” i en straffebestemmelse i straffeloven er for lite teknologisk nøytralt.

§ 9 - Etterfølgende befatning med ulovlig tilegnet data og databasert informasjon og

§ 10 - ulovlig befatning med tilgangsdata

Det må reises spørsmål om det er grunnlag for å fravike innholdet i straffelovens § 145 b som ble vedtatt på grunnlag av Delutredning I. Det må antas at straffelovens § 145 b tilstrekkelig vil omfatte de handlinger som er beskrevet i lovutkastet § 9 og § 10. Skulle det være enkelte befatningsformer som ikke rammes av innholdet i § 145 b vil det være enklere å tilføye disse befatningsformer til en nylig vedtatt lovtekst.

Det foreslås således at innholdet i straffelovens § 145 b videreføres i den nye straffelov.

§ 11- Skadelige dataprogram og utstyr

Skadelige dataprogrammer vil som regel være forskjellige former for datavirus og hackerverktøy. Slike handlinger er regulert i Europarådets konvensjon om cybercrime artikkel 6. Delutredning I forholdt seg bare til lovtiltak som var nødvendig for ratifikasjon av konvensjonen, men justisdepartementet foreslo i Ot.prp. nr. 40 (2004-2005) at straffelovens § 145 b skulle utvides til også å ramme datavirus og hackerverktøy, se side 20. Jeg slutter meg til justisdepartementets vurdering, og er enig i at det er naturlig å samle reglene i ett straffebud. Lovutkastets §§ 9-11 bør derfor samles i ett straffebud. Lovteksten i justisdepartementets lovutkast foreslås opprettholdt.

§ 12 – Selvspredende dataprogram

Lovutkastet synes unødig kompliserende. Handlingen antas å omfattes av justisdepartementets lovutkast til ny § 145 b, som foran nevnt. Det må antas at dataprogrammer som nevnt i § 12 er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer. Hvis enkelte befatningsformer ikke er omfattet får man heller tilføye disse til § 145 b.

Det foreslås at utkastet samles i et straffebud sammen med utkastets §§ 9-11.

§ 13 – Driftshindring

Europarådets konvensjon om cybercrime har i artikkel 5 om ”system interference” bestemmelse om alvorlig drifthindring av datasystemer. Det ble ikke gitt en særskilt bestemmelse som rammet slike handlinger på grunnlag av Delutredning I. Daværende datakrimutvalg fant at det ikke var nødvendig med endringer i norsk rett.

Jeg er enig i at dette nå bør gjøres, men finner at innholdet i utkastets § 13 ikke er tilfredsstillende. De handlingsformer som bør rammes av bestemmelsen er beskrevet i Europarådets artikkel 5 og bør helt eller delvis inntas i straffebestemmelsen.

§ 14- Masseutsendelse av elektroniske meldinger

Lovutkastet antas å ramme alle former for ”spam”. Disse kan ha sine legitime grunnlag i markedsføring. Det er således en nær sammenheng med de normer som er inntatt i markedsføringsloven, og bestemmelsen foreslås overført til denne lov.

§ 15- Identitetstyveri og bruk av uriktig identitet

Den såkalte ”identity theft” eller om en vil identitetstyveri er et økende problem. Personopplysninger kan komme på urette hender og brukes til å skape en uriktig identitet hovedsakelig som middel til å begå bedrageri og dokumentfalsk. Selve tilegnelsen av personopplysningene og bankkontonummer kan gjøres straffbart enten som en særskilt straffebestemmelse eller som et ledd i en bredere bestemmelse som rammer forberedelseshandlinger. Utkastets § 15 rammer bruken av uriktig identitet ved elektronisk kommunikasjon og det må reises spørsmål om forholdet til bestemmelsene om dokumentfalsk og bedrageri.

Under fremmed rett gis informasjon om enkelte internasjonale tiltak. Særlig vises til de initiativ som nå er iverksatt i EU. Det foreslås at en avventer etablering av en særskilt straffebestemmelse for bruk av uriktig identitet ved elektronisk kommunikasjon, og gjennomfører lovtiltak i samsvar med tiltak i EU.

§ 16- Kontomisbruk

Lovutkastet har nær sammenheng med bestemmelsen om bedrageri og hvis forholdet ikke i dag rammes av straffloven § 270 nr 2 bør handlingsformene tilpasses bedrageribestemmelsene. Det må også reises spørsmål om å benytte begrepet "konto" i en straffebestemmelse i straffeloven. Utkastet § 16 foreslås ikke inntatt i særskilt kapittel om datakriminalitet.

§ 17- Grovt uaktsomt datalovbrudd

Overtredelser av bestemmelsene i straffeloven rammer bare forsettlige lovbrudd, jf ny straffelov § 21. Europarådets konvensjon om cybercrime forutsetter at handlingen er straffbare når det foreligger forsett. Det foreligger ikke tilstrekkelig grunn til å fravike dette prinsipp i norsk rett. Lovutkastet § 17 foreslås ikke medtatt i kapittel om datakriminalitet.

§ 18 – Grovt datalovbrudd

Det kan være hensiktsmessig å samle de omstendigheter som gjør handlingene grove i en bestemmelse i kapittelet om datakriminalitet. De må reises spørsmål om ikke bestemmelsen bør omfatte flere alternativer som kan gjøre handlingene grove. Særlig vises til de omstendigheter som straffelovskommisjonen selv peker på, at overtredelsen er planmessig utført eller av andre grunner er særlig krenkende eller til vesentlig ulempe. Handlingen kan være planmessig utført hvis det foreligger overtredelser av mer systematisk eller organisert karakter. Overtredelsen kan være av særlig krenkende art hvis gjerningsmannen får tilgang til sensitive opplysninger.

§ 19- Lite datalovbrudd

Som foran nevnt foreslås lovutkastet tatt ut av kapittelet om datakriminalitet. Europarådets konvensjon om cybercrime forutsetter ikke at det gis en særlig straffereaksjon for mindre eller ubetydelige overtredelser. Hva som er "lite" kan være vanskelig å fastslå i datasammenheng.

Endring i ny straffelov § 7 - Handling som anses foretatt på flere steder

Bestemmelsene i ny straffelov § 7 er en videreføring av bestemmelsen i straffelovens § 12 annet ledd. Det er derfor på det rene at bestemmelsene i straffeloven kan anvendes når handlingene er begått i Norge eller resultatet er inntrådt eller fremkalt i Norge. Det vises også til avgjørelse i Rt. 2003 s.1770. Etter § 7 foreligger to gjerningssteder. Det ene hvor handlingen er begått og det andre det sted hvor virkningen er inntrådt eller tilsiktet inntrådt.

Det antas derfor ikke behov for en endring av ny staffelov § 7.

Ny straffelov kapittel 13 – Inndragning

Til forslag om endring i ny straffelov § 69 annet ledd skal bemerkes at elektronisk lagret informasjon er data og det er derfor ikke behov for tilføyelsen herunder dataprogrammer som er data.

Til forslag om endring av ny straffelov § 76 annet ledd har jeg ingen merknader.

Det er foreslått ny bestemmelse i ny straffelov § 76 a om særregler for inndragning av konto på datasystem.

Det må reises spørsmål om redigering av dette lovutkast. Det fremgår av ny straffelov § 71 at inndragning skal skje ovenfor lovbryteren.

Til mindretallets forslag om ny straffelov § 76 b – filtrering av steder på Internett, skal bemerkes at dette antas å innebære et nytt prinsipp som inneholder en form for forhåndssensur. Inndragning forusettes å gjennomføres etter at den straffbare handling er rettskraftig avgjort.

Endringer i øvrige deler av ny straffelov

Jeg har ikke vesentlige merknader til lovutkastets uttalelse om artikkel 6 i Europarådets tileggsprotokoll av 28.01.2003.

Til lovutkastets bemerkninger om ny straffelov § 26-10 bemerkes at uttrykket ”Internett” ikke er tilstrekkelig teknologisk nøytralt til bruk i straffebestemmelser.

Til skissen om enkelte endringer i reglene om dokumentfalsk bemerkes at straffelovkommisjonen på side 375 uttaler at det bør tydeliggjøres i definisjonen av dokument at elektronisk lagret informasjon omfattes. Det vises til dansk rett hvor straffelovens § 171, stk.2 er endret til følgende ordlyd:

" Ved et dokument forstås en skriftlig eller elektronisk med betegnelsen av utstederen forkynt tilkjennegivelse, der fremtreder som bestemt til at tjenes som bevis."

Til utkastet § 31-2, særregler for elektronisk signatur bemerkes at en eventuell bestemmelse i straffeloven må være i samsvar med andre bestemmelser i lovgivningen som angår elektronisk signatur.

III - Fremmed rett

Det er beklagelig at Delutredning II ikke inneholder noen oversikt eller henvisning til fremmed rett. I den globale harmonisering av lovgivning om cybercrime som nå foregår er det viktig at Norge tilpasser seg sine internasjonale forpliktelser. Lovtiltak må gjennomføres i overensstemmelse med internasjonalt godkjent standarder og prinsipper.

Jeg er ikke kjent med at det foreligger lovtiltak i andre land som tilsvarer lovutkastet i Delutredning II, og vil nedenfor redegjøre kort for enkelte trekk i den internasjonale utvikling og opplyse om tilgang til åpne kilder.

1. De forente nasjoner

World Summit on the Information Society vedtok i Tunis i 2005 etablering av lovgivning og andre tiltak om blant annet informasjonsteknologi, sikkerhet på datasystemer og nettverk og lignende. Det ble utarbeidet et dokument om cybersecurity og cybercrime. International Telecommunication Union (ITU) i Geneve har iverksatt disse tiltak. ITU gjennomfører globale konferanser og tilbud om informasjon og opplæring med fokus på tre hovedsatsningsområder, hvorav det ene er ”Harmonizing National Legal Approaches on Cybercrime”. ITU har etablert en webside: cybersecuritygateway, se www.itu.int/osg/spu/cybersecurity// .

Siste globale konferanse ble avholdt i Genève i mai 2007.

2. Europarådet

Europarådet er den mest aktive regionale organisasjon med vedtakelsen av konvensjonen om cybercrime av 2001 som en global milepæl. Den inneholder de standarder og prinsipper for lovtiltak om cybercrime som bør virke som retningslinjer for de globale lovtiltak. Europarådet avholder også årlige konferanser. Informasjon om Europarådets tiltak kan finnes på www.coe.int

3. Den Europeiske Union (EU)

EU har etter vedtak av rammebeslutningene vært noe avventende. Men i mai 2007 har EU kommisjonen sendt en særskilt kommunikasjon om felles tiltak for å bekjempe cybercrime. En utredning om fellestiltak er nå satt i gang blant annet for vurdering av lovtiltak for å bekjempe nye metoder for å begå cybercrime. Informasjon kan finnes på EU kommisjonens webside www.europa.eu

4. Andre regionale organisasjoner

Flere regionale organisasjoner gjennomfører flere tiltak for å bekjempe cybercrime. En oversikt over disse tiltak kan finnes på www.cybercrimelaw.net

5. Lovgivningstiltak i andre europeiske land

En rekke europeiske land har gjennomført lovtiltak mot cybercrime. Etter at Europarådets konvensjon ble vedtatt har blant annet følgende land gjennomført lovtiltak: Tyskland, Sverige, Island, England, Nederland, Danmark, Frankrike, Belgia, Bulgaria, Estland, Italia, Polen, Romania, i tillegg til Norge. Europarådet har anbefalt lovtiltakene i Romania som en modell for lovtiltak. Informasjon om de nye straffebestemmelser i Romania og de øvrige land kan likeledes finnes på www.cybercrimelaw.net

6. USA

USA har ratifisert Europarådets konvensjon om cybercrime uten at det var nødvendig å gjennomføre endringer av føderal straffelovgivning. Informasjon om dette finnes likeledes på www.cybercrimelaw.net

IV - Merknader til høringsuttalelsens lovutkast

1. Alminnelige merknader:

Straffelovrådet la i NOU 1985:31 til grunn at de tradisjonelle straffebestemmelser om blant annet skadeverk og dokumentfalsk var tilstrekkelig til å anvendes ovenfor handlinger begått ved hjelp av de nye teknologiske midler. Bestemmelser som kunne anvendes mot datakriminalitet ble ikke samlet i et eget kapittel i straffeloven.

Gjennom fremveksten av Internett er situasjonen i dag en annen. Straffelovkommisjonen går i Delutredning VII inn for å samle straffebud som tar sikte på beskyttelse av informasjon og informasjonsutveksling i kapittel 23. Det kan imidlertid reises spørsmål om Straffelovkommisjonen går for langt i sin samling av straffebestemmelser. Bestemmelser om brudd på taushetsplikt, brudd på bedriftshemmelighet og offentliggjøring av private forhold er straffebestemmelser som verner andre interesser. Informasjonen er ikke skaffet til veie på ulovlig måte ved uberettiget tilgang eller endring. Det er åpenbaringen av informasjonen som er det sentrale element. Det er vesentlig forskjell i de interesser som beskyttes, og som bør føre til at et eget kapittel inneholder mer sammenlignbare straffebestemmelser som er typiske for datakriminalitet.

De straffebestemmelser som bør samles i ett kapittel er slike som rammer uberettiget tilgang til data, dataavlytting, dataskadeverk, systemskadeverk, ulovlig spredning av tilgangsdata og hackerverktøy og en særskilt bestemmelse om forberedelseshandlinger til slike handlinger. Det er de samme handlinger som er omhandlet i Europarådets konvensjon om cybercrime. Hensynet til en hensiktmessig oppfølgning av våre internasjonale forpliktelser tilsier også at vi bør velge en struktur som er globalt akseptert. Elektronisk dokumentfalsk og databedrageri bør fortsatt ha sin nåværende plassering særlig av hensyn til forenkling i strukturen av straffebestemmelser. Men også de tradisjonelle bestemmelser om dokumentfalsk bør få en særskilt bestemmelse om elektronisk dokumentfalsk.

2. Alminnelige vilkår i straffebestemmelsene

Straffebestemmelsene inneholder et krav om at handlingen må være ”uberettiget”. Dette utrykket inneholder den generelle reservasjonen om at det ikke er meningen å ramme alle de handlinger som ellers går inn under straffebestemmelsene. De vanlige straffefrihetsgrunner som samtykke, nødrett og nødverge får her som ellers anvendelse. Likeledes kan handlingen være berettiget fordi den har hjemmel i lov, avtale eller annet rettsgrunnlag. Handlingen kan være lovlig foretatt av offentlig myndighet, for eksempel en forvaltningsmyndighet i staten eller av politiet. Lovlige handlinger og aktiviteter som er en del av utviklingen, design, drift og vedlikehold av datasystemer og nettverk rammes ikke. Hvis ansatte handler i strid med instrukser kan handlingen normalt være straffbar. På lignende måte kan eksterne kontraktsparter som for eksempel en lovlig bruker eller tjenestetilbyder rammes av et straffeansvar.

Beskyttelsesbrudd kan være berettiget for eksempel hvis en sikkerhetsansvarlige har fullmakt til å forsøke og forsere en passordbeskyttelse for å teste systemsikkerheten. Testing med samtykke av den berettigede for å avsløre svakheter i sikkerhetssystemet medfører ikke straffeansvar. Skyldkravet er forsett for alle straffebestemmelser. Det vises for øvrig til den nye straffelov §§ 21-23.

Straffebestemmelser rammer også de som på en eller annen måte har medvirket til handlingene, for eksempel ved planleggingen eller utførelsen. Det følger av bestemmelsen om medvirkning i den nye straffelov § 15 at et straffebud rammer også den som medvirker til at straffebudet brytes.

Forsøk på handlingen er straffbart. Etter § 16 i den nye straffelov kan den som har forsett om å fullbyrde et lovbrudd som kan medføre fengsel i ett år eller mer, og som foretar noe som er ment å lede direkte til utføringen, straffes for forsøk.

I samsvar med situasjonen blant annet i Danmark og Sverige foreslås en særskilt straffebestemmelse for forberedelseshandlinger til handlinger nevnt i kapittelet.

Hvor ikke annet er nevnt er påtalen ubetinget offentlig.

Det offentlige kan påtale de straffbare forhold uten at det foreligger noen anmeldelse eller begjæring fra noen som er fornærmet. Politiet og påtalemyndighet kan iverksette etterforskning av eget tiltak.

3. Uberettiget tilgang til lagrede data

3.1 Alminnelige merknader:

Det foreslås en videreføring av straffeloven § 145 annet ledd med en viss forenkling. Straffelovskommisjonen foreslår også å skille ut handlingene i § 145 annet ledd. Kommisjonen foreslår å opprettholde krav om et brudd på en beskyttelse eller lignende form for inntregning. Straffebestemmelsen får da også betegnelsen ” brudd på informasjonsbeskyttelse”.

Når det gjelder alternative ”uberettiget tilgang til data som overføres ved elektroniske eller andre tekniske midler” slik som beskrevet i straffeloven § 145 annet ledd, finner kommisjonen det mer naturlig å betegne dette som overvåkning og foreslår særskilte bestemmelser sammen med avlytting av telefonsamtaler. Jeg slutter med til utgangspunktet. Uberettiget tilgang til data ved avlytting under overføring ved hjelp av elektroniske midler eller andre tekniske hjelpemidler bør skilles ut som særskilt bestemmelse i utkastets § 23 a-2. Straffelovens § 145 annet ledd innebærer at det ikke lenger stilles som alminnelig vilkår at gjerningsmannen må bryte en beskyttelse for å kunne straffes. Det er tilstrekkelig at han bare skaffer seg uberettiget tilgang til andres lagrede data. Kravet om et beskyttelsesbrudd gir ikke et tilfredsstillende strafferettslig vern for privat personer, som ofte etter overgangen til trådløst kommunikasjon ikke beskytter sine data tilstrekkelig ved for eksempel å installere tilstrekkelig ”fire walls” og ”spyware protection”.

Formålet ved straffelovens § 145 annet ledd og utkastet § 23 a – 1, er behovet for å sikre datasystemer og nettverk mot uberettigede angrep. Straffebudet skal verne om datasystemenes konfidensialitet, integritet og tilgjengelighet. Samfunnets organisasjoner og enkeltindivider må kunne administrere og operere datasystemer og nettverk uforstyrret og med pålitelighet. Bestemmelsen rammer selve den rettsstridige tilgang til data eller inntrengning i et datasystem.

3.2 Tilgang til lagrede data

Uttrykket ”data” skal tolkes vidt og omfatter alle former for elektronisk informasjon. Det antas ikke nødvendig i tillegg også å medta uttrykket ”programutrustning”, idet

dette er data i dataprogrammer. Data må være lagret, og det kan foretas på alle former for lagringsmedier i et datasystem, for eksempel harddisk, disketter, og CD` og lignende. Et krav må imidlertid være at de lagrede data er maskinlesbare. Det er den uberettigede tilgang til data i datasystemer som rammes, både enkeltstående datasystemer og nettverk.

Det er den uberettigede tilgang og innsyn i data i seg selv som er straffbar. Det er tilstrekkelig at gjerningsmannen bare observerer og leser informasjonen i datasystemer. Selv om dataene bare er gjort tilgjengelige for ham uten at han tilegner seg kunnskapen eller han forstår innholdet i informasjonen, eller vet hvor informasjonen er lokalisert, er handlingen straffbar. Det er ikke noe krav om at informasjonen skal være lastet ned. Den som uberettiget skaffer seg tilgang til data ved bruk av trådløst nettverkstilgang kan straffes. Dataene må være lagret på et lagringsmedium. Hvis de er under overføring må den særskilte bestemmelse om dataavlytting få anvendelse. Men bare å sende en e-post til et datasystem er ikke å anse som ”tilgang til data”. Handlingen kan ofte synes uskyldig, men den ulovlige tilgang til data og programmer kan medføre betydelige økonomiske konsekvenser. Særlig ved mistanke om inntrengning fra hackere, kan det være nødvendig å gjennomgå datasystemene for å sikre seg mot andre følger. Det kan bety at datasystemer og nettverk vil kunne være ute av funksjon i kortere eller lengre tid.

3.3 Strafferammen

Strafferammen for uberettiget tilgang til data bør heves til bøter eller fengsel inntil 1 år, eller begge deler. Det vises særlig til at forsøk på handlingen ellers ikke vil være straffbar etter den nye straffelov § 16. Strafferammen for den uberettiget tilgang til lagrede data bør heves til bøter eller fengsel inntil 3 år hvis det foreligger skjerpende omstendigheter. Straffelovskommisjonen foreslår å innføre en særskilt bestemmelse om grovt brudd på informasjonsbeskyttelse etter samme mønster som de andre bestemmelser som kommisjonen foreslår. Enten man velger en slik løsning eller fremhever de straffeskjerpende omstendigheter i selve straffebudet kan være et lovteknisk spørsmål. Uansett hvilken løsning man velger bør de inneholde de omstendigheter som Straffelovkommisjonen fremhever. Særlig at overtredelsen er

planmessig utført eller av andre grunner er særlig krenkende eller til vesentlig ulempe. Handlingen kan være planmessig utført hvis det foreligger overtredelse av mer systematisk karakter eller organisert karakter. Skjer handlingen ved brudd på en beskyttelse bør dette også medtas.

4. Dataavlyttning.

4.1 Alminnelige merknader

Europarådets konvensjon om cybercrime inneholder i artikkel 3 en særskilt bestemmelse om ”illegal interception”. Flere land har tilsvarende straffebestemmelser som bare rammer avlytting av data under overføring. Hensynet til våre internasjonale forpliktelser tilsier derfor at Norge også bør innføre en slik særskilt bestemmelse. Avlytting av telefonsamtaler rammes av straffeloven § 145 a som er begrenset til å gi et strafferettslig vern mot avlytting av samtaler mellom personer, men ikke avlytting av data. Det er et klart behov i dag for et strafferettslig vern mot avlytting av elektronisk kommunikasjon. Det bør etableres en særskilt bestemmelse som rammer det å avlytte, oppfange eller overvåke slik kommunikasjon. Slik avlytting kan skje enten direkte gjennom tilgang til og bruk av datasystemer, eller indirekte gjennom bruk av elektronisk avlyttingsutstyr. Bestemmelsen må også ramme uberettiget oppfanging av data via elektromagnetisk stråling, for eksempel når data er rekonstruert av utstrålning fra kabler som overfører slike data. Dette er særskilt nevnt i Europarådets konvensjon artikkel 3.

Straffelovens § 145 annet ledd rammer i dag både uberettiget tilgang til lagrede data og tilgang til data under overføring. Det er naturlig og hensiktsmessig i den raske utvikling av tele- og datakommunikasjon å skille ut de straffbare handlinger som er rettet mot overføringen av data. Formålet med straffebestemmelsen er å gjøre det straffbart å avlytte eller oppfange data under overføring på en urettmessig måte. Det er de samme interesser som vernes som ved avlytting av telefonsamtaler mellom personer. Alle former for datakommunikasjon beskyttes, også ved hjelp av teleks, telefaks og lignende.

4.2 Gjerningsbeskrivelsen

Straffebestemmelsen rammer avlytting, overvåkning eller oppfanging av data under overføring til, fra eller innen et datasystem. Det forutsettes imidlertid at det er selve overføringen som er ikke-offentlig eller ikke er alminnelig tilgjengelig, og ikke selve innholdet. Selv offentlig tilgjengelig informasjon kan overføres ikke-offentlig. Ønsker partene ved en overføring av data at den skal være konfidensiell, er overføringen ikke-offentlig. Overføringer av data omfatter alle former for elektroniske kommunikasjonsmidler, enten det er ved hjelp av kabler, satellitt eller radiosignaler. At overføring av data skjer igjennom et intranett har ingen betydning. Det er her som ellers selve tilgangen til data under overføring som er straffbart, ikke om gjerningspersonen har skaffet seg kunnskap om innholdet. Den som uberettiget fanger opp data fra elektromagnetisk utstrålning fra datasystemer straffes for dataavlyttning. Strålingen vil her kunne omdannes til elektroniske data.

Avlytting av data kan gjennomføres ved hjelp av dataprogrammer som er skjult for å gjennomsøke datakommunikasjon etter hvert som de passerer, slik som på Internett. Slike programmer brukes for å få tak i informasjon, særlig passord og andre tilgangskoder som senere kan benyttes til å skaffe seg ulovlig tilgang til data. Dataprogrammene kan gjemmes som bestanddel i ellers lovlige programmer.

Bestemmelsen krever at overføringen skjer ved hjelp av elektroniske eller andre tekniske midler. Avlyttingen kan skje enten ved direkte tilgang og bruk av datasystemet, eller indirekte ved hjelp av elektronisk avlyttingsutstyr. Avlyttingen kan også omfatte opptak av overføringen. Avlyttingsutstyret kan være direkte montert på overføringskabler eller linjer, eller omfatte hjelpemidler til å avlytte, overvåke eller oppfange trådløs overføring.

4.3 Strafferammen

Straffen for overtredelse bør være bøter eller fengsel i inntil 3 år eller begge deler. Medfører handlingen betydelig skade eller ulempe, eller er overtredelsen planmessig utført eller av særlig krenkende art, eller foreligger andre skjerpende omstendigheter kan fengsel i inntil 6 år anvendes.

5. Dataskadeverk

5.1 Alminnelige merknader

Europarådets konvensjon om cybercrime inneholder i artikkel 4 en særskilt bestemmelse om ”data interference” eller dataskadeverk. Rammebeslutningen i EU har likeledes i sin artikkel 4 en særskilt bestemmelse om ulovlig inngrep i data. Flere land har tilsvarende straffebestemmelser og hensynet til våre internasjonale forpliktelser tilsier at også Norge bør innføre en slik særskilt bestemmelse.

Straffelovkommisjonen foreslår også at det inntas en bestemmelse som gir et strafferettslig vern mot uberettiget endring, sletting, eller tilføyelse av informasjon som er lagret ved elektroniske midler. Kommisjonen foreslår også her en særskilt bestemmelse om grovt skadeverk på elektronisk lagret informasjon.

En særskilt straffebestemmelse må rette seg mot forstyrrelse av lagrede data i et datasystem. Formålet med bestemmelsen er å sikre at lagrede data for samme beskyttelse mot skade som fysiske gjenstander. Forskjellen er at endringen av lagrede data bare er elektronisk lesbart og vil i seg selv ikke være forståelig for mennesket. Det vil det bare være når data gjøres tilgjengelig som informasjon.

En fil er normalt ikke slettet ved bruk av en vanlig ”delete” kommando, den er bare fjernet fra harddisken indeks inntil informasjonen blir overskrevet. Informasjonen kan gjenfinnes før den blir overskrevet, og teknologien er også utviklet til å gjenfinne informasjonen selv om den er overskrevet flere ganger. Men slik fjerning fra harddiskens indeks bør også få et strafferettslig vern. Data er gjort ubrukbar for den berettigedes formål siden lagringsmediet ikke lenger inneholder de fullstendige data. Websider kan også bli utsatt for ødeleggelser ved graffiti, pornografiske bilder, eller teksten på websiden blir endret, med spottende, hånende utsagn, eller trusler. Informasjon om varer og tjenester legges også på websider. Denne informasjonen kan endres eller slettes av uberettigede, som kan legge inn annonser for produkter som andre enn den berettigede fører, eller endre prislister som ligger på websiden.

Det er derfor naturlig at det gis en bestemmelse til vern mot uberettigede forstyrrelser av data, ved endring, sletting, tilføyelser og lignende.

5.2 Gjerningsbeskrivelsen

Gjenstanden for den straffbare handling er lagrede data i et datasystem, idet forstyrrelser av data i kommunikasjon rammes som systemskadeverk. Datasystemet kan være ett eller flere i et nettverk, men bestemmelsen rammer også endring av data i en lokal frittstående harddisk. Lagrede data vil være lagret på et lagringsmedium. Ved å endre eller slette data blir lagringsmediet påvirket slik at det ikke kan benyttes som forutsatt. Rent fysisk er lagrede data bare magnetiske impulser og den informasjon dataene representerer er selvsagt av utpreget immateriell karakter.

Den straffbare handling består i å skade, slette, forringe, endre, tilføye eller gjøre utilgjengelig eller ubrukelig, data i et datasystem. Felles for alle handlingsalternativene er at de alle er en eller annen måte å endre data på og omfatter enhver svekkelse av integriteten, tilgjengeligheten, eller den lovlige bruk av data. Selv om enkelte alternativ kan overlappe hverandre vil de normalt være selvstendige og typiske handlingsalternativer i datasystemer og nettverk.

Sletting av data kan sammenlignes med ødeleggelse av fysiske gjenstander, og foreligger når data eller dataprogrammer er slettet i sine originale eller tidligere lovlige fremtreden og blir ugjenkjennelig, selv om det er mulig å gjenopprette den. Den mest avanserte sletting kan skje ved bruk av logiske bomber som kan slette hele databaser og dataprogrammer.

Endring av data omfatter også endringer i kvaliteten av informasjonen slik den fremtrer menneskelig lesbart, enten forståelig slik som ved obskøne ord og uttrykk eller fullstendig uforståelig informasjon. Ødeleggelse eller tilgrising av websider omfattes også. Tilføyelse består i å tillegge eller øke mengden av data slik at innholdene av dataene endres. Både endring og tilføyelse kan skje.

Data kan gjøres utilgjengelige eller ubrukelige når gjerningsmannen forårsaker at de forsvinner på en eller annen måte uten å ha blitt slettet. I slike tilfeller blir muligheten for tilgang til dataene fjernet for den berettigede ved å forhindre eller avslutte tilgjengeligheten.

Skade eller forringelse er overlappende begreper, men omfatter også å gjøre data ubrukbare eller meningsløse. Skade på oversikten over passord og den muligheten den

berettigede har til å forebygge uberettigede angrep anses som skade på datasystemets sikkerhetsdata, selv om data ikke blir slettet eller endret.

Bruk av datavirus og ”trojanske hester” som sletter, endrer, eller blokkerer data i datasystemet rammes av bestemmelsen. Selv om datavirus ikke medfører skade foreligger endring eller tilføyelse, slik at eksisterende data blir endret. Selv om handlingen ikke forårsaker noen skade, men for eksempel bare viser et reklameinnslag eller lignende, vil det være en tilføyelse eller endring av data i den berettigedes datasystem. Implementeringen fører til at eksisterende data blir endret.

Trojanske hester som spyware-programmer blir ofte uberettiget plassert i datasystemer for å tre i funksjon for å overvåke alle aktiviteter når datasystemet benyttes. Det kan være et ønske om en såkalt ”online profiling” av offeret for senere bruk i reklamekampanjer ovenfor vedkommende, eller at motivet er tilgang til offerets personopplysninger eller bankkontonummeret. Handlingen er straffbar som dataskadeverk.

5.3 Strafferammen

Straffen for overtredelsen bør være bøter eller fengsel i inntil 3 år, men inntil 6 år hvis det foreligger betydelig skade eller ulempe, eller overtredelsen er planmessig utført, eller er av særlig krenkende art.

6. Systemskadeverk

6.1 Alminnelige merknader

Europarådets konvensjon om cybercrime inneholder en særskilt bestemmelse i artikkel 5 om ” system interference” . Rammebeslutningen i EU har likeledes i sin artikkel 3 bestemmelser om ulovlig inngrep i informasjonssystemer. Flere land har en særskilt straffebestemmelse som rammer alvorlige systemskadeverk. Internasjonale hensyn tilsier således at også Norge bør innføre en slik særskilt bestemmelse. Straffelovkommisjonen foreslår at systemskadeverk inntas i bestemmelsen om skadeverk på elektronisk lagret informasjon. I overensstemmelse med Europarådets konvensjon om cybercrime og tiltak i andre land, bør det etableres en særskilt

bestemmelse som rammer alvorlig påvirkning og forstyrrelser i datasystemenes og nettverkenes funksjon. Ved siden av at enhver form for funksjonalitet blir beskyttet, vil det da også bli klart at data under overføring får samme strafferettslig vern som lagret data. Det må gis et utvetydig strafferettslig vern mot handlinger som hindrer den lovlige og rettmessige bruk av datasystemer og nettverk. Bestemmelsen bør være atskilt fra bestemmelsen om påvirkning og forstyrrelse av selve de lagrede data.

Det er enhver form for funksjonalitet som er beskyttet men det kreves at datasystemet svekkes alvorlig eller vesentlig før et straffeansvar inntrer. De vanlige angrep mot datasystemer i nettverk i dag er såkalte DOS angrep. Slike angrep kan helt eller delvis lamme datasystemets funksjon, både ved lagring og kommunikasjon av data. Det kan skje ved bruk av spam, hvor offerets oversvømmes eller bombes med store mengder e-post. Store mengder fyller opp køen til servere og hindrer legitime brukere tilgang til server, og kan føre til datasystemet bryter sammen.

Motivene for å gjennomføre systemskadeverk kan variere fra eksterne angrep fra hackerere eller terrorister i cyberspace. De kan anta et stort omfang og får store konsekvenser. Som eksempel vises til nylig angrep på private og offentlige datasystemer i Estland.

Formålet med bestemmelsen er å ramme de som ved bruk eller påvirkning av data, forhindrer rettmessig bruk av datasystemer og systemer for elektronisk overføring av data. Straffebestemmelsen om dataskadeverk beskytter selve dataene, men bestemmelsen om systemskadeverk beskytter datasystemene. Det er dermed funksjonaliteten i datasystemene og nettverkene som beskyttes. Bestemmelsen rammer handlinger som hindrer den berettigedes bruk av datasystemer og systemer for elektronisk kommunikasjon. Det er integriteten, tilgjengeligheten og den lovlige bruk av datasystemer, og særlig interessene til tjenestetilbydere og brukere av telekommunikasjonssystemer som beskyttes.

6.2 Gjerningsbeskrivelsen

Bestemmelsen rammer den som uberettiget forårsaker en alvorlig hindring eller avbrytelse av driften av et datasystem. Dette kan gjøres ved å innføre eller overføre

data, ved å skade, slette, forvanske, endre, tilbakeholde eller hindre tilgang til data i datasystemet. Bestemmelsen omfatter datasystemer og nettverk av enhver art.

Det er et vilkår at handlingen må forårsake en alvorlig hindring eller avbrytelse av driften av et datasystem. Hva som skal anses som en alvorlig hindring eller avbrytelse av driften må avhenge av et skjønn. Men det er de virkelige alvorlige forstyrrelser bestemmelsen tar sikte på. Handlingen må ha en slik form, størrelse eller frekvens at den har betydelig skadelig effekt på den berettigedes eller tjenestetilbyderens evne til å bruke datasystemet eller til å kommunisere med andre systemer. Ved vurderingen må det også legges vekt på blant annet hvor stort datasystem som rammes av handlingen, hvor store økonomiske konsekvenser handlingen har, hvor varig og uopprettlig skaden er, om vitale deler hos den berettigede rammes og hvilke konsekvenser hindringen eller avbrytelsen får.

Når det gjelder de handlinger som kan forårsake den alvorlige hindring eller avbrytelse vises til merknadene under punkt 5 om dataskadeverk. Handlinger som går ut på å slette, skade, forringe, tilføye eller endre data, vil være de samme ved systemskadeverk.

Datasystemer kan som følge av disse handlinger bryte sammen for kortere eller lengre tid eller behandle data med treg eller lavere hastighet eller behandle data unøyaktig, eller unnlate nøyaktig behandling. Disse følger kan være midlertidig eller permanente, delvise eller fullstendige. Et DOS angrep kan også simuleres, slik at datasystemet reagerer ved å ikke tillate noen tilgang.

6.3 Strafferammen

Straffen for overtredelsen bør være bøter eller fengsel i inntil 3 år. Strafferammen øker til 6 år hvis det foreligger betydelig skade eller ulempe, eller overtredelsen er planmessig utført, eller er av særlig krenkende art. Særlig skjerpende omstendigheter kan foreligge hvor gjerningsmannen forårsaker en alvorlig hindring eller avbrytelse av driften av offentlige informasjonssamlinger. Det samme gjelder den kritiske infrastruktur for energiforsyning, kringkasting og telekommunikasjon. I slike tilfeller skapes omfattende forstyrrelser og representerer en alvorlig og betydelige trussel mot

offentlig administrasjon og mot samfunnsliv for øvrig, og straffelovens § 151 b kan komme til anvendelse.

7. Uberettiget spredning av tilgangsdata og hackerverktøy.

7.1 Alminnelige merknader

Straffelovens § 145 b om spredning av tilgangsdata ble vedtatt ved lov av 08.04.2005 nr 16. Det er nå straffbart uberettiget å gjøre tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem.

Justisdepartementet foreslo i sin proposisjon at bestemmelsen også skulle omfatte dataprogrammer og andre innretninger som særlig er egnet til å begå straffbare handlinger. Stortinget sluttet seg ikke til forslaget fra justisdepartementet. Flertallets begrunnelse i justiskomiteen var et ønske om ikke å kriminalisere slike handlinger, mens mindretallet ville følge justisdepartementets lovutkast.

Innretninger som datavirus og hackerverktøy har i alminnelighet intet lovlig formål, og brukes til å begå straffbare handlinger. For å begrense disse handlinger er det utvetydig nødvendig å straffesanksjonere besittelsen av datavirus og hackerverktøy, og å gjøre slike innretninger tilgjengelige for andre.

Jeg gir min tilslutning til begrunnelsen fra justisdepartementet i Ot.prp. nr 40 (2004-2005) side 18-21 og det lovutkast som ble utarbeidet.

Justisdepartementets lovutkast er inntatt som høringsuttalelsens lovutkast § 23 a – 5. Jeg viser til justisdepartementets begrunnelse som tiltres, og finner ikke grunn til ytterligere merknader i denne sammenheng.

8. Elektronisk dokumentfalsk

8.1 Alminnelige merknader

Europarådets konvensjon om cybercrime inneholder i artikkel 7 en særskilt bestemmelse om ”computer-related forgery” . Flere land har funnet det nødvendig å endre bestemmelsene om dokumentfalsk for at bestemmelsen skal omfatte annet en skriftlige tilkjennegivelser. Hensynet til våre internasjonale forpliktelser tilsier at også

Norge bør endre bestemmelser om dokumentfalsk, slik at de klart og utvetydig omfatter elektronisk dokumentfalsk.

Data som representerer informasjon kan endres eller slettes slik at informasjonen blir endret, og kan sammenlignes med forfalskning av dokumenter i tradisjonell forstand. Endringene fremtrer som logiske resultater i menneskelig lesbar form som atskiller handlingen fra dataskadeverk. Slike handlinger betegnes som elektronisk dokumentfalsk.

Elektroniske dokumenter må gis et særskilt strafferettslig vern på grunn av behovet for riktig grunnlag for rettslig relevante disposisjoner. Det er viktig å beskytte den alminnelige tillit til elektroniske dokumenters ekthet. Det er ønskelig å fastsette uttrykkelig i dokumentfalskbestemmelser at de også omfatter elektronisk informasjon.

Straffelovkommisjonen foreslår at det tas inn i kapittel 31 i ny straffelov om vern av tilliten til dokumenter og penger, en bestemmelse i § 31-1 om definisjon av falsk dokument og i § 31-2 om dokumentfalsk. Straffelovkommisjonen foreslår at det blant annet tas inn en bestemmelse som erstatter straffelovens § 182 om benyttelse av falsk dokument.

En bestemmelse om elektronisk dokumentfalsk bør innarbeides i bestemmelsen om benyttelse av falsk dokument, og høringsuttalelsens lovutkast betegner bestemmelsen foreløpig som § 31-2 a.

8.2 Dokumentbegrepet

Hvis uberettigede endringer i data skal straffes som dokumentfalsk må data som representerer informasjon også omfattes av straffelovens dokumentbegrep i straffelovens § 179. Straffelovrådet drøftet i NOU 1985:31 side 11-12 denne problemstilling og fant at data som var lagret eller bearbeidet ”ved hjelp av EDB var dokument i relasjon til straffelovens § 179”.

Slik som informasjons- og kommunikasjonsteknologien har utviklet seg bør straffelovens dokumentbegrep nå mer hensiktsmessig tilpasses dagens samfunn. Det norske dokumentbegrepet er også videre enn tilsvarende bestemmelser i de fleste land

og er derfor lite egnet i det internasjonale samarbeidet som vi forplikter oss til. Det er behov for å etablere et klart strafferettslig vern for databehandlet informasjon som erstatter skriftlige dokumenter. På samme måte som i Danmark bør det også i norsk rett uttrykkelig fastslås at bestemmelsen om dokumenter i straffeloven omfatter elektroniske tilkjennegivelser og ikke lenger knytte dokumenter opp mot gjenstandsbegrepet. Elektronisk lagrede dokumenter og elektronisk kommunikasjon med e-post erstatter i stadig økende grad kommunikasjon med skriftlig dokumenter, og dokumentet lagres nå som hovedregel elektronisk.

I forbindelse med en ny lovbestemmelse kan det reises spørsmål om å begrense det strafferettslige vern til å omfatte tilfelle hvor det er gjort bruk av elektronisk signatur. Det bør neppe være en slik forutsetning om sikkerhetskrav i de elektroniske tilkjennegivelser, men anvendelse av slik signatur vil kunne få betydning for bevisførsel. For sammenhengens skyld er det heller ikke noe krav om underskrift på tradisjonelle skriftlige dokumenter for at det skal kunne anses som et dokument.

Det er heller ikke nødvendig å opprettholde alternativet ”på annen måte”. Dette uttrykket tok opprinnelig sikte på hva som ble nedtegnet eller anbrakt ved hjelp av mekaniske midler.

Straffelovkommisjonen går i sin utredning inn for endring av dokumentbegrepet i straffeloven. Kommisjonen uttaler at det bør tydeliggjøres i definisjonen av dokument at den omfatter elektronisk lagret informasjon.

Den nye tvisteloven som trer i kraft 01.01.2008 bruker i § 26-1 uttrykket ”elektronisk lagret materiale” som likestilt alternativ med dokumenter.

Det foreslås således at definisjonen av dokument slik som den nå fremtrer i § 179 endres ved at uttrykket ”elektronisk” tilføyes som alternativ til ”skriftlig” og at uttrykket ”gjenstand” forsvinner. Det gjøres dermed utvetydig at alle bestemmelser i straffeloven som inneholder ”dokument” også omfatter elektroniske tilkjennegivelser, som for eksempel elektronisk post.

8.3 Benyttelsen av falsk dokument

Den som i rettsstridig hensikt benytter som ekte eller uforfalsket et ettergjort eller forfalsket dokument straffes for dokumentfalsk i medhold av straffeloven § 182. Både Straffelovrådet i 1985 og Datakrimutvalget i 2003 fant under noe tvil at endring eller sletting av data medførte at data ble ”benyttet”. Begrunnelsen var at databehandlingen er automatisert slik at forfalskningen og benyttelsen smelter sammen i en handling. Dette er også lagt til grunn i rettspraksis i Rt.1991 s.532.

Det er nødvendig utvetydig å sikre at elektroniske dokumenter har det samme strafferettslig vern mot forfalskning som tradisjonelle skriftlige dokumenter. På samme måten som for dataskadeverk er hensynet behovet for å verne om dataenes integritet. Men det må reises spørsmål om straffelovens § 182 slik den er utformet, på en hensiktsmessig måte tilfredsstiller disse hensyn. Det vises også til den tvil som er kommet til uttrykk både i Straffelovrådet og Datakrimutvalget. Nyere lovgivning om informasjon –og kommunikasjonsteknologi har modernisert dokument- og kommunikasjonsbegrepet, og straffelovens vern om integriteten til elektroniske data som benyttes til dokumentfalsk må også tilpasse seg utviklingen.

Straffelovkommisjonen åpner for at det bør utformes en lovtekst som tilfredsstiller prinsippene i Europarådets konvensjon artikkel 7. Denne artikkel gjør ikke straffbarheten avhengig av å benytte et dokument, men rammer selve falskhandlingene. Ved at kravet om ”benyttelse” fjernes fra gjerningsinnholdet vil en oppnå en utvetydig hjemmel for ramme den som uberettiget tilføyer, endrer, sletter eller skjuler data for at disse uautentiske data skal fremstå som autentiske og skal legges til grunn i rettslige relevante disposisjoner. Forståelsen av disse uttrykkene er den samme som ved dataskadeverk, og det vises til disse merknadene.

Elektronisk dokumentfalsk foreligger som ellers ved dokumentfalsk, når det ikke stammer fra den som angivelig har utferdiget eller avgitt det, eller dette bare delvis er tilfelle. Dokumentet kan være utferdiget eller avgitt på alle former for lagringsmedia eller kommunikasjon, som for eksempel elektronisk post. Dataene må benyttes som om de er ekte eller uforfalsket. Hvis den som utsteder informasjonen åpent tilkjennegir at dataene er falske, rammes ikke handlingen av bestemmelsen.

Skyldkravet er forsett idet gjerningsmannen må være klar over eller regne det som overveiende sannsynlig at data i det elektronisk dokument er tilføyd, endret, slettet eller skjult i et datasystem. Han må være klar over at dette fører til at de uautentiske elektroniske data fremstår som autentiske. Handlingen må som ellers ved dokumentfalsk være foretatt i rettsstridig hensikt. I dette ligger som et avgjørende krav at gjerningsmannen har ønsket å oppnå et rettslig relevant resultat.

9. Forberedelseshandlinger

Det er foran under de alminnelige merknader i I-7 redegjort for rettstilstanden når det gjelder forberedelseshandlinger i norsk rett, samt forholdet til svensk og dansk rett.

Informasjons og kommunikasjonsteknologien er i dag inne i en voldsom utvikling. En digital revolusjon med to veis kommunikasjon, nettsamfunn og informasjons- eller fildeling. Kriminelle bruker nye aktiviteter som phishing, pharming, spam, identity-theft, spyware, virus og trojanske hester, DOS-angrep også videre. Flere av disse aktiviteter brukes av kriminelle som en ren form for forberedelse til straffbare handlinger.

Den tradisjonelle lære om grensen mellom den straffrie forberedelse og forsøk på straffbare handlinger har sin vesentlige betydning i forhold til fysiske handlinger med personer og materielle gjenstander. Gjennomslagskraften i denne lære er ikke like vesentlig overfor immaterielle objekter slik som data. Forskjellen ligger på det objektive plan. Aktiviteter som phishing, pharming, botnets og spam har hovedsakelig intet lovlig formål, eller i beste fall et meget begrenset lovlig bruksområde og er særlig egnet til å benytte som hjelpemidler for senere straffbare handlinger.

Valget kan stå mellom å gi stadig nye straffebestemmelser for å verne mot stadig nye digitale eller elektroniske aktiviteter som benyttes av kriminelle, eller å vedta en straffebestemmelse som rammer forberedelse til de straffbare handlinger som er nevnt i kapittel 23a. Forberedelsen av disse handlinger bør i seg selv være straffbare. Spredning av aktivitetene til andre kan være like straffverdig. Dette bør lede til at det ikke kreves at gjerningsmannen hadde til hensikt å begå straffbare handlinger. Også

rent forsettlige overtredelser bør være straffbare når gjerningsmannen er klar over at aktivitetene er særlig egnet til å begå straffbare handlinger.

En særskilt bestemmelse om straff for forberedelseshandlinger kan øke tilliten til og bruk av elektronisk kommunikasjon. Dette vil trygge samfunnets bruk av informasjons- og kommunikasjonsteknologi.

Det foreslås i høringsuttalelsens lovutkast en straffebestemmelse som rammer enhver befatning med data i et datasystem, som er særlig egnet til å anvende som hjelpemiddel til en straffbar handling, skal straffes som forberedelse til straffbare handlinger.