NOU Norges offentlige utredninger 2007: 2

# Lovtiltak mot datakriminalitet

## Delutredning II

Utredning fra Datakrimutvalget oppnevnt ved kongelig resolusjon 11. januar 2002.
Avgitt til Justis- og politidepartementet 12. februar 2007.

Departementenes servicesenter
Informasjonsforvaltning

Oslo 2007

ISSN 0333-2306
ISBN 978-82-583-0911-3

Lobo Media AS

# Til Justis- og politidepartementet

Datakrimutvalget ble opprettet ved kongelig resolusjon 11. januar 2002. Etter mandatet skal utvalget utrede lovtiltak mot datakriminalitet. I desember 2003 avga utvalget NOU 2003: 27 «Lovtiltak mot datakriminalitet» Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi. Utredningen gjelder de endringer som var nødvendige å foreta i norsk rett for å ratifisere Europarådets konvensjon av 8. november 2001 (datakrimkonvensjonen 185 ETS). Konvensjonen er senere gjennomført i norsk rett og trådte i kraft med virkning for Norge per 1. oktober 2006.

I den foreliggende delutredning II kommer utvalget med forslag til straffebestemmelser om datakriminalitet som kan tas inn i den spesielle delen i den nye straffeloven.

Det foreligger dissens om tre spørsmål. Det ene gjelder utkast § 11 om straffbar befatning med skadelig dataprogram og utstyr (kapittel 5.7.5). Et flertall går inn for å fremme forslag om denne bestemmelsen. Det andre gjelder forslag om filtrering av steder på internett, jf. utkast § 76b (kapittel 5.13). Et mindretall går inn for å fremme dette forslaget. Det tredje gjelder forslaget om harmonisering av visse bestemmelser i straffeloven og åndsverkloven (kapittel 5.1.2 med videre henvisninger). Det er enstemmighet om at bestemmelsene bør harmoniseres og at de på sikt bør integreres slik at regelverket forenkles. Utvalget har delt seg i synet på om integreringen bør skje allerede som følge av lovforslaget som presenteres her, eller om spørsmålet bør utredes videre før det gjennomføres. Et flertall går inn for integrering som anvist i denne utredningen.

Utvalget benytter anledningen til å takke foredragsholdere på våre seminarer og andre som har hjulpet oss under arbeidet.

Oslo, 12. februar 2007

Knut Rønning
leder

Christina Christensen — Jenny Sellæg — Birthe Taraldset

Svein Willassen — Hanne P. Gulbrandsen/ Christian With

Inger Marie Sunde

# Innhold

# Kapittel 1
# Sammendrag

*Kapittel 1.* Kriminalitet hvor datatekniske hjelpemidler benyttes som verktøy for å begå straffbare handlinger rettet mot data og datasystemer, reduserer det moderne samfunnets tillit til velfungerende og sikker elektronisk kommunikasjon.

Datakrimutvalgets lovforslag er basert på en virkelighet som kjennetegnes ved at innbyggerne på kort tid har fått tilgang til et meget stort antall databaserte produkter og tjenester, og at samfunnet har blitt sterkt avhengig av datateknologien på stadig flere områder. Det er ingen grunn til å tro at denne utviklingen vil avta i årene som kommer.

Den raske teknologiutviklingen i samfunnet gjør at behovet for en dynamisk straffelovgivning som fanger opp eksisterende og nye kriminalitetstrusler er fremtredende. Datakrimutvalget er av den oppfatning at dagens regler om datakriminalitet er utilstrekkelige, og at det foreligger et reelt behov for presiseringer og en viss nykriminalisering. Den store utviklingen i teknologien fører til at også de kriminelle følger etter og tar i bruk datatekniske hjelpemidler for å begå tradisjonell kriminalitet. Utvalget fremhever videre at dette hensynet har gjort det nødvendig å gå lenger i å oppstille strafferettslig ansvar enn det som følger av minimumskravene i datakrimkonvensjonen (ETS 185) av 8. oktober 2001. Det erkjennes samtidig at utviklingen nødvendiggjør jevnlig ettersyn med lovgivningen på dette området.

Mandatet av 6. september 2005 stiller Datakrimutvalget fritt med hensyn til systematisk plassering av straffebudene, og i dag er nok erfaringen at krenkelser mot data og datasystemer reiser så mange særlige spørsmål at man er best tjent med en særregulering. Utvalget foreslår derfor å samle bestemmelsene om datakriminalitet i et eget kapittel kalt «Vern av data, databasert informasjon og datasystemer» i ny straffelov.

Datakrimutvalgets utredning har følgende hovedinnhold:

*Kapittel 2* gir en oversikt over utvalgets mandat, sammensetning og arbeid.

*Kapittel 3* gir en oversikt over samfunnsutviklingen på området, og søker å illustrere den faktiske sammenhengen mellom teknologiutviklingen og kriminalitetsutviklingen. Utvalget fremhever at utbredelsen i bruken av informasjons- og kommunikasjonsteknologi stort sett har gitt brukerne positive virkninger, men at den også har medført nye farer og trusler. Kapitlet gir en generell oversikt over noen av de vanligste formene for rettstridig adferd på området.

*Kapittel 4.* I dette kapitlet beskriver utvalget hva det legger i begrepet «datakriminalitet», og utvalget begrunner hvorfor det har valgt å foreslå særlige bestemmelser om dette fremfor å inkorporere alternativene i de øvrige straffebestemmelsene. Det fremheves at tungtveiende rettstekniske hensyn og den indre sammenheng mellom straffebudene trekker i retning av at bestemmelsene bør samles i et eget kapittel. Utvalget redegjør for de avgrensninger i mandatet som er av betydning for det foreliggende arbeidet.

Kapittel 4 gir videre et innblikk i tidligere historikk og utredningsarbeid på området, og det redegjøres for hovedlinjene i den nasjonale rettsutviklingen fra Straffelovrådets utredning i NOU 1985: 31 frem til arbeidet med ny straffelov. Videre gis det en oversikt over folkerettslige forpliktelser på området, og til slutt beskrives de sentrale rettspolitiske hensyn på området.

*Kapittel 5.* I dette kapitlet beskrives og problematiseres de rettslige hovedelementene i lovforslaget. Utvalget drøfter her sine forslag til lovmessige løsninger, og samspillet mellom de ulike bestemmelsene i lovforslaget.

Utvalget identifiserer et harmoniseringsbehov mellom åndsverkloven §§ 53a og 53c, straffeloven §§ 145 annet ledd og 145b, og straffeloven § 262. Det fremheves at det ikke anses tvilsomt at det foreligger en nær sammenheng mellom disse bestemmelsene, siden de alle gjelder uberettiget tilgang til data og handlinger som tar sikte på å tilrettelegge for uberettiget tilgang til data.

Datakriminalitetens internasjonale karakter nødvendiggjør en vurdering av lovforslagets dekning av Norges folkerettslige forpliktelser på området.

Utvalget gjennomgår datakrimkonvensjonens bestemmelser, og viser at lovforslaget dekker konvensjonen, og på enkelte områder går lengre.

Kapittel 5 inneholder generelle betraktninger om begrepsbruken og rettsstridsreservasjonen, og kapitlet inneholder de generelle merknadene til lovforslaget. Utvalget har også drøftet skyldkravet og medvirkeransvaret, samt hvorvidt tredjepersoner som tjenesteytere, betalingsformidlere, programutviklere og leverandører kan gjøres straffansvarlige.

*Kapittel 6.* I lovutkastet har utvalget valgt strafferammene for de ulike handlingene ut fra en vurdering av handlingenes straffverdighet. Til dels har utvalget tatt utgangspunkt i andre straffebestemmelser i gjeldende straffelov som man anser har tilsvarende straffverdighet. For andre handlinger – som vanskelig kan sammenlignes med bestemmelser i gjeldende straffelov – har utvalget på mer fritt grunnlag gitt et forslag til strafferamme. På tradisjonell måte velger utvalget å foreslå relativt vide strafferammer for å fange opp den ulike straffverdighet handlinger som faller innenfor samme straffebestemmelse kan ha.

*Kapittel 7.* Datakrimkonvensjonens tilleggsprotokoll av 28. januar 2003, regulerer rasistiske eller fremmedfiendtlige handlinger foretatt ved hjelp av datasystem. Utvalget vurderer hvorvidt tilleggsprotokollen er i overensstemmelse med norsk rett. Av hensyn til ytringsfriheten, går utvalget inn for at Norge bør reservere seg mot tilleggsprotokollen artikkel 6, som regulerer fornektelse, minimalisering eller positive ytringer om krigsforbrytelser eller andre forbrytelser mot menneskeheten. For øvrig finner utvalget at norsk rett er i samsvar med tilleggsprotokollen.

*Kapittel 8.* Datakriminalitet reiser spørsmål om jurisdiksjon. Det er særlig datakriminalitetens internasjonale og grenseløse karakter som får betydning både i forhold til spørsmålet om hvor en handling skal anses begått og hvorvidt vedkommende skal kunne strafforfølges i Norge. Utvalget vurderer disse problemstillingene i kapittel 8 og foreslår en presisering i straffeloven.

*Kapittel 9.* Kapitlet inneholder særmerknadene til utvalgets lovforslag.

*Kapittel 10.* Utvalget vurderer her de økonomiske og administrative konsekvenser av lovforslaget. Forslagene til endringer i straffeloven viderefører dagens straffelov på noen områder, presiserer området for det straffbare på noen punkter og utvider området på andre områder. Lovforslagene har imidlertid til felles formål å bekjempe datakriminalitet mer effektivt. Det er lagt vekt på at lovforslaget skal representere et godt verktøy for alle som arbeider med å bekjempe datakriminalitet, herunder påtalemyndigheten og domstolene. Dette kan føre til flere pådømmelser og lengre utmålt straff. Bestemmelsene vil derfor på kort sikt kunne gi økt belastning på strafferettsapparatet og føre til behov for flere fengselsplasser, men lovbestemmelsenes preventive virkning vil også kunne føre til mindre datakriminalitet og dermed samfunnsmessige besparelser.

*Kapittel 11* innholder utvalgets lovforslag, og har følgende hovedinnhold:

- Straffebud som rammer elektronisk kartlegging av sårbarheter på et datasystem (§ 2).
- Straffebud som rammer ulovlig anbringelse av utstyr eller dataprogram på eller i tilknytning til et datasystem eller elektronisk kommunikasjonsnett (§ 3).
- Straffebud som rammer ulovlig tilgang til hele eller del av et datasystem (§ 4).
- Straffebud som rammer tyveri av informasjon og data (§§ 5 og 6).
- Straffebud som rammer uberettiget endring, ødeleggelse, sletting eller skjuling av andres data (§ 7).
- Straffebud som rammer uberettiget bruk av andres datasystem eller elektroniske kommunikasjonsnett (§ 8).
- Straffebud om etterfølgende befatning med ulovlig tilegnet data og informasjon (§ 9).
- Straffebud som rammer uberettiget befatning med passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem (§ 10).
- Straffebud som rammer befatning med dataprogram eller utstyr som er særlig egnet til å begå straffbare handlinger (flertallsforslag i § 11).
- Straffebud som rammer rettsstridig befatning med selvspredende dataprogram, eller initiert spredning av slikt program (§ 12).
- Straffebud som rammer handlinger som vesentlig hindrer eller er egnet til vesentlig å hindre driften av et datasystem eller elektronisk kommunikasjonsnett ( § 13).
- Straffebud som rammer ulovlig masseutsendelse av elektroniske meldinger (spam) til mottakere som ikke har samtykket (§ 14).
- Straffebud som rammer identitetstyveri eller uberettiget bruk av uriktig identitet ved elektronisk kommunikasjon (§ 15).
- Straffebud som rammer den som med forsett om vinning uberettiget disponerer over en konto som tilhører en annen, ved å gi opplysninger til et datasystem og derved volder tap eller fare for tap for noen (kontomisbruk - § 16).

Datakrimutvalget foreslår videre endringer i ny straffelov, markedsføringsloven og åndsverkloven. Utvalget har bl.a. foreslått en skisse til integrering

av bestemmelser om datafalsk i straffelovens kapittel om dokumentfalsk og en del presiseringer i reglene om inndragning. Et flertall har foreslått at enkelte bestemmelser i åndsverkloven inkorporeres i straffeloven, og et mindretall har foreslått en lovhjemmel om filtrering av utenlandske nettsider med innhold som er straffbart i Norge.

# Kapittel 2
# Innledning

## 2.1 Datakrimutvalgets oppdrag og sammensetning

Utvalget ble oppnevnt ved kongelig resolusjon 11. januar 2002. Ifølge det opprinnelige mandatet skulle utvalget innen 31. desember 2002 avgi en delutredning om gjennomføringen av Europarådets konvensjon om IKT-kriminalitet, og deretter - innen utgangen av 2003 - avgi en ny delutredning om hvilke andre lovendringer som var hensiktsmessige for best mulig å kunne bekjempe datakriminalitet.

Utvalget avga 2. november 2003 NOU 2003: 27 «Lovtiltak mot datakriminalitet» (delutredning I). Utredningen ble fulgt opp av departementet i Ot.prp. nr. 40 (2004-2005) om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon, og resulterte i endringslov 8. april 2005 nr. 16. Loven trådte i kraft straks.

I forhold til den neste delutredningen ble det foretatt en endring av det opprinnelige mandatet. Formålet var å harmonisere forslaget til nye straffebud mot datakriminalitet med departementets arbeid med de øvrige straffebudene i den nye straffeloven. Ved Justisdepartementets brev av 6. september 2005, ble punkt 3 og 5 i det opprinnelige mandatet (gjengitt i NOU 2003: 27 side 8) erstattet, og mandatet lød som følger:

> «Utvalget skal først utrede hvilke endringer som bør gjøres i straffelovgivningen, og avgi en egen delutredning om dette innen 1. september 2006. Utvalget bes særskilt om å vurdere
> - om bestemmelsene om lovens stedlige virkeområde i den nye straffelovens alminnelige del gir hensiktsmessige avgrensninger når det gjelder ulovlig materiale på internett, jf. Ot.prp. nr. 90 (2003-2004) side 167 flg., og eventuelt foreslå særregler,
> - om data og datasystemer har et tilstrekkelig strafferettslig vern etter dagens regler, og eventuelt hvordan vernet bør forbedres,
> - om den gjeldende straffeloven i tilstrekkelig omfang og tilstrekkelig strengt straffer handlinger som begås ved misbruk av data og datasystemer, og
> - hvilke lovendringer som er nødvendige for at Norge skal kunne ratifisere tilleggsprotokollen 28. januar 2003 til Europarådskonvensjonen om IKT-kriminalitet (om kriminalisering av rasistiske og fremmedfiendtlige handlinger begått i et datasystem) [...]
>
> Der tilleggsprotokollen åpner for at statene kan reservere seg, skal utvalget dessuten vurdere om reservasjonsadgangen bør benyttes, jf. artiklene 3, 5 og 6. Selv om utvalget eventuelt går inn for at reservasjonsadgangen bør benyttes, skal utvalget likevel fremme forslag om hvordan protokollen kan gjennomføres i norsk rett uten at det gjøres bruk av reservasjonsadgangen.
>
> Utvalget skal utforme lovforslag som kan tas inn i den spesielle delen i en ny straffelov. For øvrig vises det til punkt 4 i det opprinnelige mandatet.
>
> I tillegg bes utvalget [...] om å utrede og foreslå straffeprosessuelle regler om dataavlesing, jf. Ot.prp. nr. 60 (2004-2005) side 141-142 med videre henvisninger.»

I henhold til punkt 4 i det opprinnelige mandatet, som fortsatt gjelder, skal utvalget

> «i tillegg til hensynet til samfunnsbeskyttelse vurdere rettssikkerhetsmessige aspekter og hensynet til personvern og ytringsfrihet. Ved drøftelsen av enkeltspørsmål skal utvalget gjøre rede for hvordan disse hensynene berøres og for hvordan disse hensynene bør veies mot hverandre.
>
> Utvalget skal vurdere de økonomiske og administrative konsekvensene av sine forslag, og minst ett forslag skal baseres på uendret ressursbruk, jf. utredningsinstruksen pkt. 3.1.
>
> Utvalget skal utarbeide forslag til lovtekst. Lovforslaget skal være i samsvar med Norges internasjonale forpliktelser, og utarbeides i tråd med Justisdepartementets veiledning i Lovteknikk og lovforberedelse (2000).»

I forbindelse med arbeidet med delutredning II har utvalget hatt slik sammensetning:
- Sorenskriver Knut Rønning, Sandefjord (leder)
- Advokat Birthe Taraldset, Bergen

- Statsadvokat Jenny Sellæg, Nordland statsadvokatembeter, Bodø
- Forsker Svein Willassen, NTNU, Trondheim
- Rådgiver Christian With, Datatilsynet, Oslo
- Underdirektør Christina Christensen, Samferdselsdepartementet, Oslo

Medlemmet Christian With gikk over til ny arbeidsgiver pr. 1. mai 2006. Han ble erstattet av seniorrådgiver Hanne P. Gulbrandsen fra Datatilsynet. Av hensyn til behovet for kontinuitet, samt fullføring av skriveoppgave, har Christian With likevel deltatt i resten av utredningsperioden ved å møte i utvalgsmøtene uten stemmerett.

Stipendiat Inger Marie Sunde, Universitetet i Oslo, har vært utvalgets sekretær. I tillegg til utvalgets sekretær, har cand.jur. Maria Astrup Hjort og studentene Ole Henning Nygård og Martin Rove fungert som utvalgets sekretariat.

Utvalget har også vært bistått av studentene Gemetchu Hika, Øystein Madsen, Rine Simensen og Christopher Haugli Sørensen.

Utvalget ble gitt en ny frist til 1. september 2006 med for å avlevere delutredning II. Denne fristen er i forståelse med departementet forskjøvet til februar 2007. Departementet har også samtykket i at spørsmålet om en straffeprosessuell regulering av dataavlesing utsettes til behandling i neste fase av utvalgets arbeid, se bemerkningene i kapittel 4.3.4.

## 2.2 Datakrimutvalgets arbeid

I forbindelse med arbeidet har utvalget avholdt 18 fellesmøter. Utvalget har også avholdt 2 lukkede dagsseminarer med det formål å sette utvalget inn i de utfordringer dagens høyteknologiske samfunn står overfor når det gjelder trusselbilde og kriminalitetsformer.

Det skal bemerkes at utvalget har ønsket å kartlegge lovgivningen på dette området i andre land, i og med at harmonisering av den nasjonale materielle straffelovgivning har stor betydning for et effektivt internasjonalt samarbeid. Den korte tiden som utvalget har hatt til disposisjon har imidlertid umuliggjort dette.

# Kapittel 3
# Det faktiske landskapet

## 3.1 Innledning

Lovgivningens oppgave er å regulere virkeligheten. For å regulere datakriminalitet må lovgiver ta utgangspunkt i den faktiske situasjonen i samfunnet, og her har det oppstått store endringer på grunn av utviklingen av datateknologien. En kan snakke om en revolusjon som er av like stor betydning som den industrielle revolusjon var i sin tid. Datateknologien har skapt mange nye muligheter, men også nye farer og trusler. Informasjons- og kommunikasjonsteknologien (IKT) er i dag blant samfunnets viktigste infrastrukturer. Oppstår det alvorlige problemer på denne sektoren, kan også vitale samfunnsinteresser bli skadelidende. Det er derfor viktig med en straffelovgivning som gjenspeiler dagens trusler. Men siden utviklingen er av svært dynamisk karakter, er det uansett vanskelig å sørge for at lovgivningen holder tritt med samfunnsutviklingen. Det antas derfor å være behov for et jevnlig ettersyn med straffelovgivningen på dette området.

Trusselbeskrivelsen nedenfor, sammen med de rettslige utgangpunktene i kapittel 4, danner bakteppet for de lovforslag som utvalget fremmer.

## 3.2 Teknologi og samfunnsutvikling

### 3.2.1 Internett og utfordringene ved å regulere internett ved lovgivning

Fremveksten av internett har hatt stor betydning i samfunnet. Internett har gitt nesten ubegrensede muligheter til kommunikasjon og informasjonsformidling. Dette har igjen åpnet for en utvikling i samfunnet som for noen tiår siden var utenkelig. Enorme mengder informasjon kan publiseres ett sted i verden, for å være tilgjengelig et helt annet sted i løpet av sekunder. Internett brukes daglig av folk over hele verden.

Det foreligger betydelige utfordringer tilknyttet straffeforfølgning på tvers av landegrenser for forbrytelser foretatt ved bruk av internett. Det er ofte vanskelig å identifisere forbryterne, og dersom man klarer det, vil de ofte forsvare seg med at handlingene er utført i at annet land der serveren stod, eller at de befinner seg i et land hvor de ikke kan forfølges eller som ikke vil utlevere vedkommende til et annet land. Gjennom internetts relativt korte historie har det likevel vist seg at kontroll av internett og forfølgning av lovbrytere på nettet er mulig.

Samfunnsliv og økonomi er avhengig av velfungerende teknologiske løsninger. Sikker og effektiv bruk av datateknologi har betydning på alle plan i samfunnet, privat, i næringslivet, i den offentlige forvaltning og for å sikre statens interesser i et internasjonalt perspektiv. Teknologiutviklingen er en drivkraft i den såkalte globaliseringsprosessen, og medfører at aktører på alle plan i samfunnet kan kommunisere og samhandle internasjonalt.

Utviklingen i globale nett åpner opp for nye forretningsmuligheter, markeder og bedriftskonstellasjoner. Internett som global arena gir historisk sett unike utfoldelsesmuligheter for aktørene.

Norge har som et velstående og modernisert samfunn lagt stor vekt på å bygge ut og tilgjengeliggjøre elektroniske kommunikasjonstjenester. Regjeringen har i den såkalte Soria Moria-erklæringen en uttalt ambisjon om å sikre alle husstander, private og offentlige virksomheter et bredbåndstilbud i løpet av 2007.

### 3.2.2 Utbredelse og bruk av datamaskiner og internett

Kilden for de tall og beregninger det er vist til i det følgende er «Nøkkeltall for informasjonssamfunnet 2005» av Statistisk Sentralbyrå (SSB), med mindre annet er angitt.

*Blant private*

Privatpersoners bruk av datamaskin og internettbaserte tjenester har økt markant de siste årene. Tall viser at Norge ligger helt i europatoppen både når det gjelder handel, bruk av finansielle tjenester og tilegnelse av aviser eller nyheter på internett.

Av landets husstander har 64 prosent internettilkobling, og to tredjedeler av disse er bredbånd. En stor andel av de som ikke har datamaskin eller

internettilkobling i egen husstand, oppgir at de har tilgang til internett andre steder.

Handelen på internett øker. I 2005 foretok 55 prosent av befolkningen handel på internett. Det er mest populært å handle varer og tjenester som reiser, innkvartering, billetter og bøker. Det skjer også en stadig økende omsetning av film, musikk, klær, sportsartikler, elektronisk utstyr, datamaskiner og programvare på denne måten.

77 prosent av brukerne som har benyttet internett i løpet av en periode på tre måneder, har benyttet dette til finansielle tjenester som nettbank. Tall fra Norges Banks årsrapport for betalingssystemer 2005, viser at det foreligger omlag 3,1 millioner nettbankavtaler Norge.

86 prosent av internettbrukerne bruker e-post. 75 prosent leser aviser og lignende på internett.

Bruken av direkte kommunikasjon over nettet er tiltagende. Det er populært, særlig blant yngre, å kommunisere gjennom ulike pratekanaler og gjennom programmer som gjør det mulig å skrive direktemeldinger til hverandre. (Yahoo Messenger og MSN er eksempler på slike tjenester.) Ved slik kommunikasjon er det også vanlig å opptre under pseudonym (se mer om pseudonymbruk i kapittel 5.3.5). Med programmer som Skype, MSN og lignende, kan man også snakke sammen (lydsamtale) kostnadsfritt, dersom man har mikrofon og høyttaler. Med et webkamera kan man se den man kommuniserer med. Til enhver tid er det millioner av brukere over hele verden på slike tjenester.

### *I næringslivet*

Bedriftenes verdiskaping er i stadig større grad støttet av databaserte systemer. Mer enn 90 prosent av norske foretak med flere enn ti sysselsatte har internettilkobling. Dessuten tas stadig flere forskjellige online-tjenester i bruk i næringslivet.

I 2004 hadde en femtedel av foretakene omsetning via internett. Total verdi av denne omsetningen var på 59 milliarder kroner, dersom man ser bort fra bank- og finansnæringens omsetning. Til tross for at det er vanskelig å fastslå slike tall med sikkerhet, er det klart at det har skjedd en stor økning i omsetning via internett.

For større globale foretak med installasjoner og avdelinger i forskjellige deler av verden har internett ført til en vesentlig kostnadsbesparing. Tidligere gikk ofte kommunikasjon mellom de ulike avdelingene og installasjonene innad i foretaket gjennom linjer/kabler som foretaket disponerte. Nå foregår det alt vesentlige av slik kommunikasjon over internett, dvs. på en infrastruktur som ikke er kontrollert av selskapene selv. Det har også vanlig at medarbeidere som har hjemmekontor eller er på reise, kobler seg opp mot bedriftens datasystemer via internett. Den økte konnektiviteten har store fordeler, men også ulemper i form av økt risiko for at uvedkommende kan få tilgang til bedriftens datasystemer.

Internett har også medført større grad av sentralisering av datasystemene i større bedrifter. Ved bruk av internett kan instruksjoner gis fra en sentral og utføres av personale andre steder. Det er også mulig med en fullstendig automatisering, slik at store produksjonsmaskiner styres fullstendig fra en sentral uten menneskelig involvering på selve produksjonsanlegget. Med stadig større båndbredde og raskere overføring er det få begrensninger i hvilke instruksjoner som kan gis i form av tekst, bilder, lyd, video osv. Dataoverføring knyttet til styrings- og produksjonssystemer skjer gjennom såkalte virtuelle private nettverk (VPN), som er et kryptert samband over internett.

Dette utviklingstrekket er omtalt i utredningen NOU 2006:6 «Når sikkerheten er viktigst» på side 45:

> «Innenfor kritiske samfunnsfunksjoner vokser også utfordringene etter hvert som prosesser som tidligere ble kontrollert innenfor lukkede systemer, i økende grad kobles til Internett. Et eksempel er styrings- og prosessystemer som blir koblet opp mot administrative systemer, som igjen blir koblet opp mot Internett for å imøtekomme publikums behov for informasjon. Det er også økende bruk av teknologiske løsninger hvor eksempelvis driftspersonale plassert utenfor eget nettverk har behov for å knytte seg direkte opp mot egne prosessystemer, og hvor Internett er koblingen mellom bruker og det interne nettverket. Denne utviklingen kommer hovedsakelig som et resultat av krav til økt effektivitet og fleksibilitet.»

Næringslivets bruk av elektroniske tjenester i kontakt med offentlige myndigheter har økt. Siden 2003 har andelen foretak som benytter internett til å rapportere opplysninger til det offentlige økt med over 150 prosent. Omtrent 60 prosent av alle foretak benytter nå elektronisk rapportering til det offentlige.

Man kan skaffe seg tilgang til datasystemer over nett, for eksempel over internett eller ved direkte fysisk pålogging (man sitter ved maskinen som man skaffer seg tilgang til). Ikke bare sikkerhetstiltak i nettet og på datasystemene, men også fysisk skjerming av maskinparken, er viktig for datasikkerheten. Selv om en bedrifts datasystem ikke er tilknyttet internett på noen måte, er det sår-

bart for uønsket atferd siden det kan være mulig å ta seg inn til de fysiske maskinene. Det vises til fremstillingen i kapittel 3.5.11.

*I det offentlige*

Det er et mål fra sentrale myndigheter at mer av kommunikasjonen med det offentlige skal foretas elektronisk. Regjeringen har skissert den ønskede fremdriften på dette området i planen «eNorge 2009 – Det digitale spranget», som blant annet inneholder planer om at alle relevante tjenester skal være tilgjengelige over internett i portalen «Altinn» innen utløpet av 2008. Også prosjektet MinSide, som skal være en personlig sikkerhetsportal for myndige borgere, er en del av myndighetenes satsing på dette området. Målet er at tjenester som søknad om barnehage, byggetillatelse, skattekort, dagpenger m.v. skal være tilgjengelige via denne portalen. Statistiske opplysninger viser at halvparten av befolkningen i en periode på tre måneder har benyttet internett ved kontakt med det offentlige.

I likhet med de fleste private bedrifter, har nesten alle offentlige etater egne nettsider. Her informeres publikum om etatenes tjenester, kontaktinformasjon og tilknyttet regelverk. Nesten alle kommuner og fylkeskommuner benytter seg av elektronisk baserte informasjons- og journalsystemer. Et flertall har elektronisk saksbehandling, og for en rekke av disse sakene er papirdokumenter fullstendig utelatt. Innen alle deler av den offentlige virksomhet viser tallene en økende bruk av elektronisk baserte tjenester og internett.

Den rettslige reguleringen ligger i dag i forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) av 25. juni 2004 nr. 988. Forskriften er gitt med hjemmel i forvaltningsloven og esignaturloven (se kapittel 3.2.5 i underkapitlet om elektronisk signatur og elektronisk sertifikat). Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen.

### 3.2.3 Nærmere om mobiltelefonbruk

Også bruken av mobiltelefon har økt de siste årene. Ved utgangen av 3. kvartal 2006 var det ca. 4,966 millioner mobilabonnenter i Norge. Dette medfører at det er flere mobilabonnementer enn personer i Norge, med 106 abonnementer per 100 innbyggere (Tall fra Post- og teletilsynet: «Det norske telemarkedet 3. kvartal 2006»). I underkant av 93 prosent av husholdningene har mobiltelefon. I 3. kvartal 2006 snakket mobilkundene gjennomsnittlig 134 minutter per måned, sendte 87 sms (tekstmeldinger) og 2 mms (multimediameldinger).

Tallene gjenspeiler at mobiltelefonen ikke lenger bare benyttes til taletelefoni. Nyere mobiltelefoner er et godt eksempel på at digitaliseringen og den tekniske utviklingen har ført til en sammensmelting av telekommunikasjon, informasjonsteknologi og kringkasting (konvergens). Mobiltelefonen har fått en rekke nye bruksområder og kan for eksempel brukes til sending av sms/mms, som kamera, den gir tilgang til internett, kan brukes som mp3-spiller, radio, mobil-tv og til å betale regninger. Videre arbeides det med løsninger hvor SIM-kortet i mobiltelefonen skal brukes som identifikator for elektronisk signatur (se kapittel 3.2.5). Med slik utvidet bruk av mobiltelefonen blir sikkerhetsaspektet av stadig større betydning.

### 3.2.4 Bruk av betalingskort og elektroniske banktjenester

Betaling ved bruk av betalingskort har økt markant de siste årene. Stadig flere aktører tilbyr sine kunder å betale for varer ved bruk av slike kort uten å belaste gebyr.

Ifølge tall fra Norges Bank, var det ved utgangen av 2005 utstedt hele 7,9 millioner betalingskort i Norge. 3 millioner av disse er rene kreditt-/faktureringskort som Diners, MasterCard o.l., 4,8 millioner er såkalt kombinerte kort som inneholder flere ulike tjenester (det vanligste er en debet-del, BankAxept, og et internasjonalt betalingskort, eksempelvis VISA). Det finnes også omlag 100 000 rene BankAxept-kort. Totalt sett er det utstedt i overkant av 12,7 millioner slike betalingsfunksjoner på betalingkort i Norge.

Det ble totalt registrert 864 millioner korttransaksjoner i 2005. Det var en økning fra året før på ti prosent. Verdien av disse transaksjonene var samlet på 485,8 milliarder kroner. Det kan nevnes at andelen av kontantuttak over skranke sank i 2005, hvilket kan sees i sammenheng med den økende betalingsformidlingen ved bruk av ulike betalingskort.

Ved utgangen av 2005 var det 2184 minibanker i Norge. Antallet minibanker var stigende frem til 2003, men har etter dette vært relativt stabilt. Det ble i 2005 registrert 98,7 millioner kontantuttak i minibank i Norge med en total verdi på 112 milliarder kroner.

Det var ved utgangen av 2005 registrert 105 482 betalingsterminaler i Norge, dvs. slike som anvendes i butikker m.v. for å kunne betale med kort. Det ble registrert over 722,3 millioner

transaksjoner via disse terminalene, til en samlet verdi av 327 milliarder kroner. I disse tallene ligger også kontantuttak i forbindelse med varekjøp. Det ble foretatt 135,9 millioner slike kontantuttak til en samlet verdi av 49,4 milliarder kroner i 2005.

### 3.2.5 Elektronisk identifikasjon

*Innledning*

Skal man ta ut penger på postkontoret, må man identifisere seg med gyldig legitimasjon, for eksempel pass eller bankkort. Også i den elektroniske verden er identifikasjon mange ganger nødvendig. Det er mange måter å identifisere seg på elektronisk. Eksempler på dette er pinkoder og passord. Normalt må man oppgi både brukernavn og passord for å logge seg inn på datasystemet til en virksomhet. Dersom påloggingen for eksempel skjer fra hjemmekontor over internett, kan identifiseringsprosedyrene være mer omfattende.

For å logge inn på betalingstjenester eller andre tilgangskontrollerte tjenester på internett benytter man et brukernavn og passord som man har fått tildelt. Dette gjelder for eksempel abonnementstjenester som en nettavis eller Lovdata. Skal man ta ut penger i en minibank, bruker man bankkortet kombinert med en pinkode for identifikasjon. Ved bruk av nettbank identifiserer man seg ved brukernavn og passord. I dag opereres det både med faste passord og passord som skiftes ut for hver gang det er brukt (engangspassord). En moderne måte å identifisere seg på er ved hjelp av elektronisk signatur. Dette er meget nyttig ved avtaleinngåelser som skjer elektronisk, og beskrives i neste avsnitt.

Kriminelle vil ofte misbruke andres elektroniske identitet, for eksempel brukernavn og passord for å komme inn på et datasystem, eller kredittkortnummer og sikkerhetskode ved nettbaserte transaksjoner. Det er grunn til å forvente at kriminell aktivitet på dette området vil øke.

*Elektronisk signatur og elektronisk sertifikat*

Elektronisk signatur er data som påføres en elektronisk melding eller et dokument, og som entydig identifiserer den som har laget meldingen/dokumentet. Metoden er basert på asymmetrisk kryptering (se neste avsnitt) kombinert med et elektronisk sertifikat. Det elektroniske sertifikatet er utstedt av en tredjepart (såkalt tiltrodd tredjepart (TTP)) som innestår for identiteten til innehaveren av sertifikatet. Sertifikatet bidrar til at en mottaker kan stole på at en melding med elektronisk signatur virkelig er fra den som utgir seg for å være avsender. Elektronisk signatur kan derfor benyttes som autentiseringsmetode (bekrefte at en melding kommer fra en bestemt avsender).

Elektronisk signatur er i utgangspunktet en ren teknisk løsning, men i lov om elektronisk signatur (esignaturloven) av 15. juni 2001 nr. 81 er det gitt lovregler som støtter bruken av slik signatur med sikte på å likestille rettsvirkningene med bruken av en alminnelig håndskreven signatur. Esignaturloven er basert på direktiv 1999/93EF av 13. desember 1999 om et rammeverk for elektronisk signatur. Loven skiller mellom kvalifisert elektronisk signatur og annen elektronisk signatur. Ifølge esignaturloven § 6 har en kvalifisert elektronisk signatur samme rettsvirkning som en alminnelig underskrift. Det bestemmes videre at også vanlig elektronisk signatur kan ha slik rettsvirkning.

I Norge har noen få private aktører tatt i bruk teknologien for inngåelse av finansieringsavtaler med mer. Bruken må forventes å være i sterk vekst. Utviklingen på dette området vil medføre at samhandel vil skje mer lettvint, hurtigere, sikrere og mer effektivt.

For nærmere informasjon om elektronisk signatur vises det til Jansen og Wiese Schartun: «Informasjonssikkerhet», Fagbokforlaget 2005 side 87-93 og 149-171, Inger Marie Sunde «Lov og rett i cyberspace» Fagbokforlaget 2006 kapittel 2.2.3.5 og Ot.prp. nr. 82 (1999-2000).

*Offentlig nøkkel kryptering (PKI)*

Elektronisk signatur er som nevnt basert på bruk av asymmetrisk kryptering, også kalt offentlig nøkkelkryptering. Den teknologi som tilrettelegger for bruken kalles PKI («Public Key Infrastructure»). Asymmetrisk kryptering går ut på at brukerne har et dobbelt sett nøkler, dvs. en offentlig og en privat nøkkel. Disse nøklene er innbyrdes korresponderende. Den private nøkkelen er hemmelig og beholdes av innehaveren, mens den offentlige er tilgjengelig for den annen part. Metoden kan benyttes til å bekrefte identiteten til avsender. Esignaturloven støtter og regulerer bruk av offentlig nøkkel kryptering.

PKI er utførlig omtalt blant annet i Adams og Lloyd: «Understanding PKI», Atreya, Hammond, Paine, Starrett og Wu: «Digital Signatures», og Feghhi og Williams: «Digital Certificates».

BankID og BuyPass er de to største aktørene på dette området i Norge. De leverer teknologi for elektroniske signaturer og utsteder ulike elektroniske sertifikater. Antall BankID-sertifikater steg fra 4 566 i 2004 til 405 608 i 2005. BuyPass eies av Posten (gjennom Ergo Group) og Norsk Tipping.

På selskapets nettsider fremgår det høsten 2006 at man forventer to millioner brukere av BuyPass-kort ved utgangen av 2006. I dette tallet er spillerkort fra Norsk Tipping inkludert.

Esignaturloven inneholder en straffebestemmelse i § 21. Denne gjelder overtredelse av regler som er vesentlige for å utøve et effektivt tilsyn med at loven etterleves, dvs. regler som sikrer PKI. Utvalget finner derfor ingen grunn til å gå nærmere inn på straffebestemmelser om dette. Bestemmelsene gjelder imidlertid ikke falske eller forfalskede elektroniske signaturer eller elektroniske sertifikater. Dette behandles i forbindelse med reglene om dokumentfalsk i kapittel 5.9. Her behandles også forfalskning av elektroniske dokumenter med elektronisk signatur. Esignaturloven inneholder heller ingen bestemmelser om bruk av en annens elektroniske signatur som også kan anses som en form for identitetstyveri.

## 3.3 Utviklingen av datakriminalitet

### 3.3.1 Innledning

Utviklingen som er skissert i de foregående avsnitt viser at Norge er avhengig av en velfungerende elektronisk infrastruktur. Denne avhengigheten som vil fortsette å øke, har medført økt oppmerksomhet om betydningen av å sikre mot feilfunksjoner, misbruk, kriminelle anslag, og terror. Sårbarhetsutvalgets utredning NOU 2002: 24 «Et sårbart samfunn», fulgt opp i Innst. S. nr. 9 (2002-2003), har gått inn på denne problemstillingen. Arbeidet er blant annet videreført i utredningen NOU 2006: 6 «Når sikkerheten er viktigst».

Det er vanskelig å uttrykke den delen av kriminalitetsutviklingen som har sammenheng med teknologiutviklingen i form av troverdig statistikk. Dette har flere årsaker. For det første foreligger et registreringsproblem. Antall anmeldelser av straffbare forhold rettet mot datasystemer og infrastruktur er trolig svært lite i forhold til det antall kriminelle handlinger som faktisk begås. Dette kan skyldes at tilfeller av datakriminalitet ikke blir oppdaget, at de ikke blir gjenkjent som datakriminalitet eller at man av ulike årsaker ikke ønsker å anmelde forholdene. I mørketallsundersøkelser utført av Næringslivets sikkerhetsråd, Økokrim og Senter for informasjonssikring for 2001 og 2003, ble forekomsten av datakriminalitet i norske virksomheter kartlagt. Ved bruk av et spørreskjema sendt et antall bedrifter, ble virksomhetene bedt om å rapportere antall tilfeller av datakriminalitet i henholdsvis 2001 og 2003. Begge undersøkelsene konkluderte med at antall tilfeller som ble anmeldt var svært lite i forhold til antall tilfeller som virksomhetene faktisk hadde oppdaget. Årsakene varierte; blant annet gjaldt de at virksomheten ikke trodde forholdet var straffbart, at man fryktet dårlig omdømme som følge av at saken kunne bli kjent på grunn av straffeforfølgningen og at man mente at politiet hadde for liten kompetanse til å behandle denne type saker.

Mørketallsundersøkelsene foretok også en sammenligning av nivået av datasikkerhetstiltak som var gjennomført i virksomhetene og antall hendelser som ble oppdaget. Denne sammenligningen viste (både i 2001 og 2003) at sammenhengen mellom sikkerhetstiltak og oppdagede hendelser var proporsjonal: Virksomhetene som hadde sterke sikkerhetstiltak rapporterte flere hendelser enn virksomhetene som ikke hadde så sterke sikkerhetstiltak. Undersøkelsene konkluderer med at det neppe kan være tilfelle at virksomheter med høyt datasikkerhetsnivå i utgangspunktet utsettes for flere datasikkerhetshendelser. I stedet peker man på at virksomheter med høyt sikkerhetsnivå vil ha bedre muligheter til å oppdage datasikkerhetshendelser som faktisk finner sted. Hovedkonklusjonen i mørketallsundersøkelsene er således at det sannsynligvis finner sted mange hendelser som aldri blir oppdaget.

I forhold til tradisjonell kriminalitet har datakriminalitet en forholdsmessig stor andel kriminalitetsformer som etter sin art er vanskelig å oppdage. Tyveri av en gjenstand er for eksempel lett å oppdage, ved at gjenstanden er borte. Datatyveri ved kopiering av data er derimot et forhold som bare blir oppdaget dersom man foretar nøye undersøkelser av datasystemet, eller eventuelt oppdager at datamaterialet er på tyvens hånd. Tilsvarende gjelder det for andre former for datakriminalitet, slik som datainnbrudd, datamodifikasjon, dataavlytting og informasjonstyveri at gjerningen i utgangspunktet kan være svært vanskelig å oppdage. Mange av disse kriminalitetsformene vil bare bli oppdaget dersom man leter aktivt etter dem, og det på en innsiktsfull måte.

Det er derfor sannsynlig at en stor andel av den datakriminalitet som begås, skjer i det skjulte. Trolig er det slik at de mest alvorlige forholdene er de som er mest profesjonelt utført. Disse forholdene vil også være vanskeligst å oppdage, ettersom gjerningspersoner med høyere grad av profesjonalitet vil ha lettere for å gjennomføre handlingen på en slik måte at den blir vanskelig å oppdage. Det er derfor svært vanskelig å gi et tallfestet bilde av kriminalitetsutviklingen innenfor datakriminalitet, ut over å peke på at teknologiene som er utsatt for

datakriminalitet er blitt mye mer alminnelig i bruk i løpet av de siste tiårene.

### 3.3.2 Typetilfeller av motiv

Ut fra avdekkede tilfeller av datakriminalitet, samt tilgjengelig informasjon fra miljøene de tilhører, er det mulig å fremstille en oversikt over typetilfeller av motiv og å si noe om hvem som er gjerningspersonene. Man bør imidlertid utvise forsiktighet med å tillegge type gjerningsperson for stor vekt. Når datakriminalitet avdekkes er det som regel ved at det oppdages på stedet der gjerningen har skjedd. Et datainnbrudd vil for eksempel som regel oppdages hos den fornærmede ved at man oppdager at uvedkommende har skaffet seg adgang til systemet. I et slikt tilfelle kan man ikke vite noe mer om gjerningspersonen enn hva man finner ved analyse av den angrepne maskinen. Det kan riktignok avdekkes informasjon om gjerningspersonens fremgangsmåte, hvilke verktøy som er benyttet og liknende, men dette sier ikke nødvendigvis noe om gjerningspersonens intensjoner. Det er bare i tilfeller hvor man faktisk klarer å spore handlingen tilbake til en gjerningsperson at man kan avgjøre hva gjerningspersonens intensjon egentlig har vært. Dette er viktig å ha i bakhodet ved en analyse av hvem som vanligvis begår datakriminalitet. Det er ikke sikkert at den gjerningspersonstypen som dominerer i avdekkede saker er den det er størst grunn til å frykte.

### 3.3.3 Spenning

Den type motiv som har vært avdekket i flest datakrimsaker til nå gjelder ønsket om spenning. Gjerningspersonene har til felles at de i utgangspunktet ikke har noe motiv om profitt, hevn eller andre personlige motiv for sin virksomhet. Virksomheten starter gjerne med at man ønsker å finne ut hva som er mulig, hvor lett det er å gjennomføre datakriminalitet som for eksempel datainnbrudd. Når man så opplever spenningen som følger med det å fritt kunne undersøke andres datasystemer, lese andres e-post og filer, får man lyst å oppleve mer spenning og utforske andre datasystemer.

I slike saker starter gjerningspersonen gjerne med å utforske hva som kan oppnås ved hjelp av verktøy og metoder han leser om på internett. Kartlegging og datainnbrudd er derfor typisk de innledende handlingene i slike tilfeller. I starten innehar vedkommende gjerne ikke kompetanse til annet enn å laste ned bestemte typer skannere og exploits (se kapittel 3.4.1 og 3.4.2), samt å kjøre disse mot sårbare systemer på internett. Fordi denne typen gjerningspersoner ofte er unge (gjerne gutter), er en vanlig betegnelse på dem «script-kiddies». «Script» er en form for dataprogram. Betegnelsen speiler at personen ikke er i stand til å lage dataprogrammer selv, men bruker programmer som er lastet ned fra andre. Virksomhet av denne typen har en bratt læringskurve og man skal ikke holde på med det lenge før man selv er i stand til å gjennomføre mer avanserte aktiviteter som for eksempel å lage skannere og ormer.

Status er et viktig element i disse sakene. Ikke sjelden hører gjerningspersonen til et miljø der det finnes flere personer som begår samme type handlinger. I tilfelle vedkommende startet på egen hånd, vil det uansett ikke ta lang tid før han finner likesinnede. Ofte finner kontakten sted via internett. I denne sammenhengen har chattesystemet Internet Relay Chat (IRC) spilt en sentral rolle gjennom de siste 15 årene. Systemet ser ut til å fortsatt være det foretrukne systemet i dette miljøet. Status i miljøet kan komme til uttrykk på mange måter. Har man for eksempel skaffet seg tilgang til en exploit (se kapittel 3.4.1) som ingen andre har, vil dette gi spesiell status. Spesiell kunnskap gir også status i miljøet. Den som kan besvare andres spørsmål om metoder og teknikker vil raskt få en spesiell posisjon. Videre kan man få status som følge av hvilke datamaskiner man har skaffet seg tilgang til. Således vil selve maskinnavnet vedkommende opererer med på IRC kunne gi spesiell status. Det finnes eksempler på at norske gjerningspersoner har opptrådt på IRC fra datamaskiner med vertsnavn som slutter på «.gov» og «.mil». Dette har åpenbart gitt spesiell status i miljøet, idet slike datamaskiner tilhører henholdsvis USAs administrasjon (.gov) og USAs forsvarsorganisasjon (.mil).

Videre er det en fordel for personer som tilhører et miljø på IRC å kontrollere flest mulig datamaskiner. Årsaken til dette er at kanaler på IRC kontrolleres av dataprogrammer (bot) som ved å være koblet til forskjellige IRC-tjenere kobler seg til en bestemt kanal og kontrollerer denne. Botene er koblet sammen i et nettverk. Siden det kan være nødvendig med mange boter for å kontrollere en IRC-kanal, er den som setter opp botnettverket som regel avhengig av å begå datainnbrudd på mange maskiner for å skaffe seg tilgang til maskiner der botene kan kjøres. Den som kontrollerer en kanal kan bestemme hvem som får lov til å oppholde seg på kanalen og hvem som får lov å skrive ting til kanalen. Den som kontrollerer kanalen kan således blant annet kaste ut dem han ikke liker, og bestemme at de ikke får lov å komme inn igjen. Det er åpenbart et mål for personer i dette miljøet å

kontrollere IRC-kanaler. I tilfelle man selv ikke kontrollerer noen kanal, kan man forsøke å overta andres IRC-kanaler ved å begå datainnbrudd på maskinene som kontrollerer kanalen, eventuelt å hindre dem fra å faktisk kontrollere kanalen ved å organisere tjenestenektangrep mot dem (se kapittel 3.4.9). Både for å holde på egne kanaler, og for å kunne gjennomføre angrep med siktemål å ta over andres kanaler, er det en fordel å kontrollere flest mulig datamaskiner. Dette har motivert deltakerne i disse miljøene til å gjøre datainnbrudd på flest mulig datamaskiner. Hvilke datamaskiner man gjør datainnbrudd på spiller ikke så stor rolle. Hovedsaken er at man kan kjøre programmer der som kobler seg til en IRC-kanal eller som angriper andre programmer med samme formål.

Siden deltakere i IRC-kanaler etterhvert blir kjent med hverandre og i større grad identifiserer seg med hverandre, blir det etter hvert dannet grupperinger i form av nettverk av deltakere som har kontakt. Slike grupperinger kan være mer eller mindre faste og kan bestå av forskjellige personer i forskjellig alder bosatt i forskjellige land, som ikke har noe annet til felles enn tilknytningen til den bestemte IRC-kanalen. Likevel kan identifiseringen med grupperingen bli sterk nok til at det noen ganger oppstår konflikter mellom forskjellige grupperinger. Slike konflikter kan utarte til en slags krig der grupperingene forsøker å overta hverandres kanaler for å ødelegge for hverandre. Siden våpnene i en slik «krig» består i å angripe hverandres botnettverk, er det mange uskyldige parter som blir rammet. Botene kjører jo på datamaskiner som gjerningspersonene tidligere har gjort datainnbrudd på og som tilhører organisasjoner eller personer som ikke har noe med IRC-krigen å gjøre. Som følge av angrepene kan alle disse innehaverne av datamaskinene få blokkert sin tilknytning til internett fordi den fylles av data som er en del av den pågående «krigen». Det finnes nok mange slike tilfeller der offeret har opplevd at internettforbindelsen har blitt ubrukelig for kortere eller lengre tid uten at man noen gang fant ut hva som traff dem.

Selv om gjerningspersonene i denne kategorien som regel ikke ønsker å ødelegge for innehaverne av datamaskinene, er det klart at det kan bli følgen likevel. Videre kan det i seg selv være ødeleggende at gjerningspersoner i denne kategorien har lav kunnskap om datasystemets rettmessige bruk. Gjerningspersonen kan for eksempel slette data han ikke skjønte betydningen av i forsøk på å fjerne spor etter datainnbruddet. En slik hendelse kan få betydelige konsekvenser for innehaveren av datamaskinen.

### 3.3.4 Hevn

Som ved tradisjonell kriminalitet, kan hevn være et motiv ved datakriminalitet. Selv om hevn til dels kan sies å være motiv i forbindelse med «krigene» som er omtalt i forrige avsnitt, er nok hevnmotiv mer utbredt i forbindelse med personlige relasjoner og relasjoner i arbeidsforhold. Ønske om hevn kan gi seg utslag i at man publiserer eller sprer ufordelaktig informasjon om andre på internett. Men også ren datakriminalitet som for eksempel datainnbrudd, tjenestenektangrep og selvspredende progammer kan være motivert av ønske om hevn. Dette kan ramme gjerningspersonens tidligere arbeidsgiver eller andre som gjerningspersonen føler seg forulempet av.

### 3.3.5 Profitt

Profitt er som ved all annen kriminalitet også et mulig motiv ved datakriminalitet. Det er lett å tenke seg hvordan man kan oppnå profitt ved å begå datainnbrudd på andres datamaskiner for å stjele informasjonen som ligger lagret der. Slik informasjon kan benyttes til å oppnå profitt. For eksempel kan informasjonen som er lagret på datasystemet være bedriftshemmeligheter som konkurrenter kan utnytte til å oppnå profitt. Eksempler på slik informasjon kan være produktbeskrivelser, regnskapstall og ikke minst markedsstrategier og konkurrentanalyser. Det finnes imidlertid ennå ikke mange kjente eksempler på at dette har skjedd. Det kan dog tenkes at dette er en type kriminalitet som ikke er så lett å avdekke.

Gjennom etableringen av et stort og i utgangspunktet legalt marked for informasjonsmegling, er det skapt en mekanisme for prissetting av informasjon slik at den økonomiske verdien kommer konkret til uttrykk. En bivirkning er at det gir et incitament for omsetning av informasjon skaffet til veie på ulovlig måte. Datakriminelle metoder kan være meget aktuelle både for å skaffe til veie slik informasjon og for å begå informasjonsheleri.

Det finnes mange eksempler på forsøk på å profitere på andres data/informasjon ved at ansatte har tatt med seg informasjonen ut av virksomheten. Det typiske tilfellet er at en ansatt kopierer med seg data fra virksomheten før vedkommende slutter. Dataene kan senere benyttes som forretningsgrunnlag ved oppstart av egen virksomhet eller i forbindelse med at vedkommende blir ansatt i en annen konkurrerende virksomhet. Slike hendelser har meget stort skadepotensiale for den virksomhet som blir offer for dette.

Tilfeller av datakriminalitet hvor profitt er motivet inkluderer også mange tilfeller av tradisjonell kriminalitet hvor dataverktøy er benyttet. Internettbedragerier er klassiske tilfeller av dette. Man bestiller for eksempel varer i falskt navn, benytter falskt kredittkortnummer eller sender ut e-post som skal lure andre til å sende penger. Denne typen datakriminalitet ser ut til å øke betydelig i omfang. For ytterligere omtale av slike tilfeller vises det til drøftelsen i kapittel 3.5.

### 3.3.6 Propaganda

I en del tilfeller har det vist seg at datakriminalitet har vært motivert av gjerningspersonens politiske ståsted. Målet med handlingen kan være å få frem et politisk budskap. Frem til nå har det vist seg at personene som utfører dette som regel har røtter i miljøet som er omtalt under kapittel 3.3.3. Det kan være at personen tilhører et miljø som forfekter et spesielt politisk synspunkt og ønsker å få frem budskapet til et bredere publikum. Metodebruken er den samme som det er redgjort for tidligere.

Det typiske eksempelet på spredning av politisk propaganda ved hjelp av datakriminalitet er såkalt «defacement». Gjerningspersonen foretar her datainnbrudd på en datamaskin som inneholder en webtjener. Deretter byttes forsiden på webtjeneren ut med en ny side som inneholder et budskap som gjerningspersonen ønsker å få frem. Hensikten med dette er å få frem budskapet til flere og til andre grupper enn det ellers ville nådd frem til. Det er også en demonstrasjon av at gjerningspersonen har klart å trenge seg inn på dataserveren, noe som skal vise styrken til grupperingen som forfekter det syn budskapet inneholder.

En annen type handling som også gjerne forbindes med slikt motiv, er tjenestenektangrep mot datamaskiner tilhørende politiske motstandere. Som diskutert i kapittel 3.4.9, er slike angrep svært vanskelige å spore eller stoppe. Det er derfor et yndet verktøy for å skape vanskeligheter for politiske motstandere, særlig blant mer militante grupperinger. Også i slike tilfeller synes det å være typisk at det er personer tilhørende miljøet omtalt i kapittel 3.3.3 som faktisk gjennomfører angrepene.

Fra det overnevnte kan en gå videre til å oppstille en hypotese om at terrorister vil benytte tjenestenektangrep i stor utstrekning for å nå sine mål. Det er på det rene at det foreligger potensiale for slik utnyttelse i terrorvirksomhet. Derimot foreligger det ikke pålitelig informasjon om at det skjer i dag. Det er på det rene at terrorister har utnyttet internett i sin virksomhet, men da først og fremst som en kanal for informasjon og kommunikasjon. Fra NOU 2006: 6 «Når sikkerheten er viktigst», hitsettes følgende betraktninger fra side 45:

> «Det har hittil ikke vært påvist noe koordinert eller vidtrekkende nettverksangrep som har truet samfunnets funksjonsdyktighet. Likevel kan det ikke avvises at det økende antall av tilsynelatende tilfeldige nettverksangrep i noen tilfeller er initiert av terrorgrupper.
>
> [...]
>
> Uoppdagede sårbarheter vil til enhver tid utgjøre en trussel, avhengig av hvem som oppdager sårbarhetene og dermed muligheten til å utnytte dem. Man kan tenke seg en meget alvorlig situasjon dersom noen finner en alvorlig sårbarhet og i tillegg gjør en grundig planlegging av hvordan den skal utnyttes før den oppdages og korrigeres (Et såkalt Zero-Day Attack).
>
> [...]
>
> Det har så langt vært vanskelig å forestille seg at kritiske samfunnsfunksjoner som vannforsyning, strømforsyning, kraftforsyning og lignende kan rammes katastrofalt på grunn av terror i form av logisk angrep fra utsiden alene, uten at det også er etablert noen form for støttespillere på innsiden. På grunn av den allerede innebygde sikkerheten, er et fullstendig fjernstyrt terrorangrep med katastrofale konsekvenser mindre sannsynlig. Ikke desto mindre skal man være oppmerksom på de stadig sterkere koblingene som skjer mellom prosessystemer og Internett.
>
> Det er i prinsippet mulig å trenge seg ulovlig inn i IT-systemer som fjernstyrer kritisk infrastruktur og kritiske samfunnsfunksjoner, men det er ikke uten videre enkelt å skulle overta styringen uten at dette oppdages av det ordinære driftspersonellet. Det er en utbredt oppfatning at det er enklere å bruke eksplosiver for å skade kritisk infrastruktur og kritiske samfunnsfunksjoner, enn å ta kontrollen over et datastyringssystem.»

### 3.3.7 Etterretning

Selv om det ikke foreligger noen bekreftede hendelser der informasjonskrigere har spilt en rolle, er det klart at også slike utgjør en mulig trussel. Informasjonskrigere er grupper som er organisert av en fremmed stat for å kunne utføre informasjonskrigføring, herunder angrep/etterretning via datanettverk. Angrepene kan rette seg mot militære installasjoner, samfunnets infrastruktur eller mot private bedrifter som er viktige for samfunnet.

Det skal være bekreftet at flere land har etablert evne til å offensivt utføre dataangrep mot andre land (Sunde 2006 «Lov og rett i cyberspace» kapittel 2.3.3). Hvorvidt slike angrep kun vil spille en rolle i eventuelle fremtidige kriger, eller om slike metoder også vil benyttes i fredstid, gjenstår å se. Fremmede staters eventuelt organiserte offensive dataangrepsvirksomhet vil trolig skille seg vesentlig fra mange av de andre aktørene med tanke på evne til å opptre med lav oppdagelsesrisiko og lav grad av sporbarhet. Dersom bare en liten del av de datasikkerhetshendelsene som skjer blir avdekket (jf. mørketallsundersøkelsene, se kapittel 3.3.1), er det svært lite sannsynlig at angrep fra fremmede stater vil være blant disse. Trolig er det derfor slik at dersom fremmede stater benytter dataangrep mot oss, er aktiv etterretning vår eneste sjanse til å avdekke dette.

## 3.4 Trusler mot datasystemer

### 3.4.1 Inntrengning i datasystemer

Inntrengning i datasystemer kalles vanligvis for datainnbrudd. Dette er en handling som innebærer at gjerningspersonen skaffer seg adgang til et datasystem hvor vedkommende ikke har rettmessig adgang. Adgangen innebærer at vedkommende får tilgang til data som er lagret på datasystemet, og vanligvis også tilgang til å kjøre programmer på systemet. Slike programmer kan eventuelt modifisere på dataene som er lagret på systemet. Et datainnbrudd innbærer altså en urettmessig tilgang som kan ramme datasystemets innehaver både ved at dataene som er lagret på systemet blir kjent for uvedkommende (konfidensialitet), ved at dataene som er lagret på systemet blir endret urettmessig (integritet) og at systemet som sådan kan bli belastet slik at det blir mindre brukbart for den rettmessige innehaveren (tilgjenglighet). Datainnbruddet er handlingen som gir gjerningspersonen tilgang til å foreta slike ytterligere handlinger på datasystemet. Et datainnbrudd har derfor ofte karakter av en handling som på en eller annen måte bryter sperrer som er satt til å verne om systemet. I det følgende behandles ulike former for datainnbrudd. Gjennomgangen er ikke uttømmende. I kapittel 5.6.2 drøfter utvalget lovtiltak mot datainnbrudd. Datainnbrudd etterfølges ofte av informasjonstyveri eller datatyveri og/eller at inntrengeren beskadiger målmaskinen ved å endre data på denne. Lovtiltak mot dette drøftes i kapittel 5.5.2 og 5.6.3.

*Passordinnbrudd*

En vanlig form for datainnbrudd er passordinnbrudd. I slike tilfeller har gjerningspersonen skaffet seg brukernavn og passord, eller andre tilsvarende tilgangsdata til en bruker som har rett til å bruke systemet. Disse opplysningene kan være skaffet på urettmessig vis, for eksempel ved dataavlytting eller passordknekking, se kapittel 3.4.6 og 3.4.7, men det kan også tenkes at opplysningene i seg selv er skaffet på rettmessig vis, likevel slik at gjerningspersonen ikke er berettiget til å bruke dem. Det kan for eksempel tenkes at en annen person har gitt opplysningene uoppfordret, se også kapittel 5.3.3.

Selve datainnbruddsgjerningen er ved passordinnbrudd karakterisert ved at gjerningspersonen logger seg på datasystemet med tilgangsdataene. Dermed får han samme tilgang til datasystemet som den rettmessige brukeren hadde, og kan kjøre programmer, lese, slette og endre filer på datasystemet. Påloggingen kan skje lokalt, ved at gjerningspersonen bruker tastatur og skjerm som er koblet til det aktuelle datasystemet. Det er også mulig å koble seg til datamaskinen ved hjelp av datanettverk og logge seg på med brukernavn og passord, for eksempel ved bruk av systemer for fjernpålogging, slik som Telnet, Secure Shell, Remote Desktop og liknende. Slik pålogging kan utføres fra alle andre datamaskiner som er tilknyttet samme datanettverk. For datamaskiner som er tilknyttet internett er det altså mulig å koble seg til maskinen fra alle andre datamaskiner som er tilknyttet internett, med mindre det er foretatt spesielle tiltak for å beskytte mot dette (brannmur eller tilsvarende). Slike beskyttelsestiltak ville i så fall også sperre mot rettmessig bruk av fjerninnlogging på systemet.

Passordinnbrudd ved fjernpålogging er en meget vanlig form for datainnbrudd. Det er velkjent at det i visse miljøer utveksles brukernavn/passord og andre tilgangsdata som man har skaffet seg. Har man først skaffet seg adgang til et datasystem, kan denne adgangen utnyttes til å fremskaffe brukernavn og passord til dette og andre datasystemer (se om bakdør, sniffing og passordknekking i kapittel 3.4.3, 3.4.6 og 3.4.7). Disse tilgangene kan selvsagt benyttes til nye datainnbrudd, men de kan også benyttes til å utveksle informasjon med andre som driver med det samme. På den måten kan man skaffe seg tilgangsdata til helt andre maskiner enn man hadde fra før og kan benytte disse til nye datainnbrudd.

*Sårbarhetsinnbrudd*

Alle dataprogrammer inneholder feil som ikke var tilsiktet fra programmereren. Det er ikke mulig å lage et fullstendig feilfritt dataprogram, like lite som det er mulig å skrive en bok som ikke inneholder noen typografiske, syntaktiske eller faktiske feil. Slike feil kalles gjerne «bugs». En bug omtales som en sårbarhet dersom den utløser en feilfunksjon som kan utnyttes bevisst til å fremkalle en utilsiktet virkning i dataprogrammet. Å utnytte sårbarheten bevisst til å fremkalle den utilsiktede virkningen kalles «exploit», etter engelsk «to exploit» – å utnytte. Slike sårbarheter oppstår vanligvis i dataprogrammer som forventer inndata fra brukeren. Dersom programmet ikke sjekker inndataene godt nok, kan det være mulig å fremkalle en utilsiktet virkning i programmet ved å sende bestemte inndata som programmet ikke forventer. Hvis inndataene er laget på en spesiell måte, kan den utilsiktede virkningen være at vedkommende som sender inndataene får urettmessig tilgang på datasystemet.

Den mest vanlige formen for sårbarhetsinnbrudd er utnyttelse av overflytssårbarheter. Denne type sårbarheter oppstår i programmer hvor et minneområde med begrenset størrelse er satt av til å håndtere inndataene og programmet ikke sjekker inndataenes lengde. Dersom brukeren av programmet tilfører mer inndata enn det som får plass i det avsatte minneområdet, vil dataområdene i minnet etter det avsatte området bli overskrevet av inndataene. Dette kan utnyttes ved at inndataene kan inneholde programkode som gir brukeren tilgang på datasystemet med samme rettigheter som det utnyttede dataprogrammet.

Utnyttelse av en sårbarhet i et dataprogram er i utgangspunktet en avansert operasjon som krever at man nøye analyserer målprogrammets virkemåte og beregner nøyaktig hvilke inndata som må gis for å oppnå den tilsiktede effekten. Resultatet er en metode som bare vil virke mot ett bestemt målprogram, og som regel bare en versjon av dette. Det vanlige er at man lager et nytt dataprogram som inneholder de dataene som må sendes til målprogrammet for å utnytte sårbarheten. Et slikt program kalles en «exploit». Som det fremgår, benyttes uttrykket «exploit» både om metoden og programmet som anvendes. Etter at exploiten er laget, vil man ved å kjøre exploiten mot et målprogram kunne utnytte sårbarhetene i dette uten å måtte bry seg med hvilke data som faktisk sendes.

Det skilles mellom lokale exploits og fjernexploits. Forskjellen mellom disse er hvilke programmer som rammes av exploiten. Lokale exploits kan i prinsippet utnytte sårbarheter som finnes i hvilket som helst lokalt program på et datasystem. Det er imidlertid lite hensiktsmessig å utnytte sårbarheter i et dataprogram uten at man på den måten skaffer seg privilegier på systemet som man ikke hadde fra før. Det vanlige ved bruk av lokale exploits er derfor at man utnytter sårbarheter i lokale systemtjenester som har privilegier tilsvarende systembrukeren. Ved å kjøre en slik exploit kan en lokal bruker som i utgangspunktet ikke har tilgang til andre brukeres programmer og data, skaffe seg fullstendige systemprivilegier og få full kontroll over hva som foregår på datasystemet, herunder lese og endre andres data.

Fjernexploits kjøres mot tjenester på andre datamaskiner som er tilknyttet samme datanettverk. Hvis FTP-tjenerprogramvaren på maskin A for eksempel inneholder en bestemt sårbarhet, kan en bruker på maskin B kjøre en exploit mot denne. Utvekslingen av data mellom exploiten og målprogrammet foregår i dette tilfellet over nettverket som knytter de to datamaskinene sammen. På denne måten kan vedkommende som kjører exploiten, få full tilgang til alle data og systemressurser på maskin A, noe han i utgangspunktet ikke var berettiget til.

Bruk av fjernexploits mot andres datasystemer er en meget vanlig metode for å begå datainnbrudd. Datamaskiner som er tilkoblet internett som tilbyr tjenester, er meget utsatt for dette. Ved å foreta skanning (se kapittel 3.4.2) kan en gjerningsperson avdekke hvilke programmer (med versjonsnummer) som kjører på en målmaskin tilknyttet internett. Dersom han har en exploit som virker mot denne programversjonen, kan han kjøre denne og straks få kontroll over målmaskinen. Både kartleggingen og selve kjøringen av exploiten kan som regel skje fra en hvilken som helst annen datamaskin tilknyttet internett.

En av årsakene til at sårbarhetsinnbrudd er vanlig, er at det finnes offentlig tilgjengelige databaser over kjente sårbarheter og tilhørende exploits. Dette gjør det mye lettere å utføre datainnbrudd for personer som ikke innehar den nødvendige kompetansen til å lage exploits selv. Det eneste man må gjøre er å finne ut hvilken programvare som kjører på målmaskinen, og om det finnes noen offentlig tilgjengelig exploit for den. Dersom dette finnes, kan man bare laste den ned til sin egen maskin og deretter kjøre den for å begå datainnbruddet.

Man kan så spørre hvorfor slike databaser finnes, idet de åpenbart bidrar til økt datainnbruddsvirksomhet. Den vanligste årsaken som oppgis av operatørene av databasene er at exploits også er viktige sikkerhetsverktøy. Den eneste måten å

avdekke om en sårbarhet virkelig eksisterer, er å kjøre en exploit mot den. Ved å kjøre alle kjente exploits mot sine egne systemer, kan systemoperatører sikre seg at det ikke finnes kjente sårbarheter som gjør at man vil bli utsatt for datainnbrudd. Dessuten kan leverandører av dataprogrammer distribuere oppdateringer av programvaren som hindrer utnyttelsen av vedkommende exploit, og sikkerhetsprogrammene kan oppdateres tilsvarende. Databasene over exploits er således en kilde til informasjon om hvilke sårbarheter som finnes på systemer. Det er en utbredt oppfatning at eksistensen av databaser over exploits er en del av et «økosystem» på internett som gjør det lettere å sikre datasystemer som virkelig trenger å være sikre. En bieffekt er imidlertid at exploits blir lettere tilgjengelig for dem som ønsker å gjøre datainnbrudd i andre systemer. Straffetrusselen for datainnbrudd representerer en nødvendig motvekt til «fristelsen» som exploits-databasene utgjør for potensielle gjerningspersoner. Den strafferettslige tilnærming til befatning med exploits som sådan, er drøftet i kapittel 5.7.5.

*Trojaner*

Metoden for datainnbrudd som er beskrevet under avsnittet om sårbarhetsinnbrudd, er en teknisk metode for å få målmaskinen til å kjøre programkode som er skrevet av angriperen. En alternativ metode for å gjennomføre dette er å forlede en rettmessig bruker av maskinen til å kjøre programkode som er skrevet av angriperen. Dette kan gjennomføres ved å lage et program som gir seg ut for å være et nyttig program, men som i tillegg til (eller i stedet for) nyttige funksjoner inneholder programkode som gir gjerningspersonen tilgang til datamaskinen. Et slikt program kalles en trojansk hest, eller en trojaner. En vanlig virkemåte er at programmet når det blir kjørt av offeret, åpner en tilgang til målmaskinen som ikke var der fra før. Dette kalles en «bakdør» (se kapittel 3.4.3). Denne tilgangen kan angriperen så benytte for å skaffe seg tilgang til maskinen.

Opphavet til begrepet trojansk hest finnes i Homers Illiaden, hvor grekerne overvant byen Troja ved hjelp av list. Etter lengre tids beleiring av Troja, trakk grekerne seg tilbake. Etter dem stod det igjen en stor trehest. Trojanerne var naturlig nok nysgjerrig på hesten og trillet den inn i byen. Om natten kom greske krigere som hadde gjemt seg inne i hesten ut og åpnet portene slik at den greske hæren kunne innta byen.

På internett finnes det ferdige trojanere som man kan laste ned, konfigurere og koble sammen med nyttige programmer som man kan sende til et utvalgt offer, for eksempel via e-post. De mest avanserte av disse (for eksempel Back Orifice og SubSeven) inneholder funksjonalitet som lar angriperen utføre en rekke funksjoner på offerets datamaskin, for eksempel lese filer, overvåke skjermbildet, avlytte rommet med datamaskinens mikrofon eller hente frem pornografi i en nettleser.

### 3.4.2 Elektronisk kartlegging i form av skanning

I forkant av et datainnbrudd foregår det som regel en kartlegging i den hensikt å finne sårbarheter som kan utnyttes. Slik kartlegging kalles gjerne «skanning». Målet med skanningen er å finne sårbarheter som kan utnyttes til å begå datainnbrudd. Man kan skille mellom «breddeskanning» og «målskanning» etter formålet med kartleggingen.

Ved breddeskanning tar gjerningspersonen for seg et område av nettadresser og sjekker alle for en bestemt sårbarhet. Dette gjøres ved å la et dataprogram (en skanner) kontakte alle adresser og undersøke om den bestemte programvaren som innholder en sårbarhet finnes på de aktuelle maskinene. Dette er en aktuell fremgangsmåte dersom man har skaffet seg en exploit som utnytter en bestemt sårbarhet, og ønsker å benytte denne til å skaffe seg uberettiget tilgang til et datasystem uten at det spiller så stor rolle hvilket datasystem man utnytter. Ønsket om tilgang kan skyldes behovet for lagringssted, for eksempel for piratvare, bruk av systemet som springbrett for videre skanning/datainnbrudd, eller rett og slett å undersøke om det finnes noe spennende på datasystemet. På internett er det i praksis uproblematisk å foreta breddeskanning av titusener av andre maskiner i løpet av relativt kort tid, noe som ofte vil gi resultat i form av at man finner en eller flere maskiner som man kan gjøre datainnbrudd på. Dette er derfor en relativt vanlig fremgangsmåte.

Ved målskanning tar gjerningspersonen for seg en bestemt adresse og sjekker hvilke tjenester som kjører på denne, i håp om å finne en eller flere tjenester som inneholder sårbarheter. Portskanning er en form for målskanning. Ved portskanning tar skanneren kontakt med alle 65536 inngangene (portene) på en måldatamaskin, for å undersøke om det finnes noen tjenester. Resultatet er en liste over alle tjenester som kjører på datamaskinen. Etter at portskanning er gjennomført kan man foreta ytterligere undersøkelser for å finne ut om noen av tjenestene som kjører på maskinen inneholder sårbarheter.

Det finnes også mellomformer mellom breddeskanning og målskanning. Man kan for eksempel tenke seg at gjerningspersonen har valgt ut en organisasjon som han vil angripe. Det er da naturlig å starte med en breddeskanning av alle maskiner i organisasjonen for å finne den letteste veien inn. Dersom det viser seg at en maskin er mye lettere å komme inn på enn de andre, vil det være naturlig å gjøre datainnbrudd på denne først. Ofte vil man få tilgang til en del informasjon på en slik maskin som gjør det lettere å gjøre ytterligere datainnbrudd.

### 3.4.3 Tekniske endringer på et målsystem

Når en gjerningsperson har gjort datainnbrudd på en datamaskin, kan det være ønskelig å gjennomføre en del endringer på systemet for å unngå å bli oppdaget, og for å sikre tilgangen. Siden man ved datainnbruddet har skaffet seg full kontroll over målmaskinen, er det fullt mulig å endre dens virkemåte ved å bytte ut programvare eller på annen måte modifisere data for å nå disse målene.

Et relativt vanlig tiltak er å bytte ut systemets egen programvare for overvåkning av aktiviteter på maskiner, med modifiserte versjoner som skjuler gjerningspersonens egen aktivitet. Et slik sett med modifisert systemprogramvare kalles et «rootkit». Når et effektivt rootkit er på plass, vil det ikke lenger være mulig for maskinens rette innehaver å se hvilke programmer (prosesser) som kjøres av inntrengeren, og forbindelser til nettverket som skyldes inntrengeren vil heller ikke vises. Det er også mulig for et rootkit å filtrere systemets logging slik at aktiviteter som skyldes inntrengeren ikke blir loggført i systemloggene.

Videre er det nokså vanlig å lage en ny tilgang til systemet som ikke var der fra før. Dette kalles en «bakdør», fordi det er en inngang til systemet som den rettmessige innehaveren ikke kjenner til. En bakdør kan opprettes på flere måter. Den enkleste måten (som også har høyest oppdagelsesrisiko) er rett og slett å legge til nye brukere på maskinen. Gjerningspersonen kan da skaffe seg tilgang ved normal fjerninnlogging som beskrevet under avsnittet om passordinnbrudd. En annen mye brukt metode er å legge til ny systemprogramvare som åpner en tjeneste (port) mot internett som ikke ble tilbudt tidligere. Den nye tjenesten kan kreve passord av den som prøver å koble seg til, eller den kan slippe andre rett inn uten passordbeskyttelse. Det er også mulig å modifisere eksisterende systemprogramvare slik at de gir tilganger på måter de ikke har gjort før. For eksempel kan man tenke seg å modifisere innloggingsprogrammet slik at det slipper inn hvem som helst som oppgir brukernavn «sesamsesam». En slik endring vil være svært vanskelig å oppdage for den rettmessige innehaveren av systemet.

Det er vanlig ved datainnbrudd at bakdører opprettes for å sikre videre tilgang til datamaskinen for det tilfelle at den rettmessige innehaveren skulle oppdage og fjerne sårbarheten. Faktisk er det også relativt vanlig at gjerningspersonen fjerner selv sårbarheten som gjorde at han opprinnelig fikk tilgang. Dette tjener to formål. For det første blir det mindre risiko for å bli oppdaget; hvis en systemadministrator oppdaget en sårbarhet kunne det også tenkes at han foretok undersøkelser for å avdekke om noen hadde utnyttet den. For det annet hindrer det at andre får urettmessig tilgang til den samme maskinen, noe som ville medføre økt oppdagelsesrisiko og mindre eksklusivitet.

At det er relativt vanlig ved datainnbrudd å foreta endringer som nevnt over, har betydning for hvordan man bør forholde seg hvis man oppdager datainnbrudd. Det er ikke tilstrekkelig å fjerne den opprinnelige sårbarheten, for det er sannsynlig at det kan finnes andre bakdører til systemet. Å oppdage slike bakdører er en vanskelig oppgave. Det er svært mye systemprogramvare på dagens operativsystem, og å finne ut hvilket program som er endret, kan være som å lete etter nålen i høystakken. Dette kan innebære mye arbeid. Datainnbrudd kan derfor få betydelige konsekvenser for den som er angrepet selv om gjerningspersonen ikke har slettet noen data eller gjort andre skadelige endringer i dataene som er lagret på maskinen.

### 3.4.4 Innholdsendringer av data

En berettiget frykt i forbindelse med datainnbrudd er at gjerningspersonen foretar innholdsendringer i dataene som er lagret på datasystemet. Teknisk sett er ikke dette forskjellig fra endringene som er behandlet under forrige avsnitt, både dataprogrammer og andre data er lagret på lagringsmediet på datamaskinen og kan fritt endres av den som har fått urettmessig tilgang.

Det hevdes iblant at det mest alvorlige som kan skje ved et datainnbrudd er at alle data blir slettet. Ved bruk av sikkerhetskopi er det imidlertid mulig å sikre seg mot slik datatap, som jo kan forårsakes av andre grunner også, for eksempel diskkrasj. Det kan være vel så alvorlig om data blir endret eller lagt til, men i så lite omfang at det ikke blir oppdaget. Dersom heller ikke datainnbruddet blir oppdaget, er det sannsynlig at den endrede informasjonen vil inngå som en del av

informasjonsgrunnlaget, og også etter hvert bli en del av sikkerhetskopien av systemet. Selv dersom datainnbruddet blir oppdaget, er det ikke sikkert at dataendringen blir oppdaget i opprydningsprosessen.

Mørketallsundersøkelsen 2003 hadde som hovedresultat at kun en mindre andel tilfeller av datakriminalitet ble avdekket, og videre at kun en mindre andel av disse ble anmeldt. Dette gir grunn til å frykte at det kun er tilfellene hvor gjerningspersonene gjør større endringer som blir oppdaget. Tilfeller hvor gjerningspersoner bare har gjort subtile endringer er etter all sannsynlighet ikke oppdaget, selv om dette kan ha svært store konsekvenser. Det kan for eksempel være tale om manipulering med regnskapstall som kan gi feil beslutningsgrunnlag og føre til endringer i aksjekursene i børsnoterte selskap.

Det er her grunn til å legge til at det ikke bare er personer som har skaffet seg adgang ved datainnbrudd som kan foreta urettmessige innholdsendringer på et datasystem. Slike handlinger kan også foretas av personer som har rettmessig tilgang til dataene, for eksempel ansatte.

De lovgivningsmessige konsekvensene av situasjonen som er behandlet i kapittel 3.4.3 og 3.4.4, drøftes i kapittel 5.6.3.

### 3.4.5 Tyveri av data

Når det har vært begått datainnbrudd, frykter man også at gjerningspersonen har kopiert konfidensielle data som er lagret på datasystemet, og bruker dem til egne formål. Kopiering av data kan også gjøres urettmessig av noen som har fysisk tilgang til vedkommende datasystem.

Urettmessig kopiering av data representerer en alvorlig trussel. Ettersom kopiering ikke medfører noen endring av dataene slik de ligger lagret på originalsystemet, er kopiering i seg selv en handling som medfører liten oppdagelsesrisiko. Dataene, og informasjonen de representerer, kan imidlertid ha stor verdi, og urettmessig utnyttelse kan få store konsekvenser. Man kan for eksempel tjene betydelige beløp på å kjenne til regnskapstall i børsnoterte selskaper før de foreligger offentlig. Informasjon om politiske beslutninger, for eksempel et statsbudsjett, er også eksempel på informasjon som potensielt har meget stor verdi før den er offentliggjort.

Det vises til den videre behandlingen i kapittel 5.5.2.

### 3.4.6 Dataavlytting

Mange datatekniske hjelpemidler kan anvendes til å foreta avlytting. En datamaskin har til en viss grad mulighet til å fange opp det som skjer i dens omgivelser. Slik avlytting kan utføres av den som har tilgang til å kjøre programmer på en datamaskin. Dette gjelder altså både en datamaskins rettmessige innehaver og andre som måtte ha skaffet seg tilgang til datamaskinen via datainnbrudd.

Det er fullt mulig å kjøre programmer som avlytter rommet datamaskinen står i, dersom en mikrofon er tilkoblet datamaskinen (noe som er relativt vanlig på laptop-maskiner). Videre kan rommet videoovervåkes dersom maskinen er tilknyttet et kamera. Det er også mulig å kjøre et program som fanger opp og lagrer alle tastetrykkene på en datamaskin (såkalt «tastetrykksregistrator», eller på engelsk «key stroke logger»). Dette kan forøvrig også utføres ved å plassere en fysisk enhet på kabelen mellom tastaturet og selve maskinen. Sistnevnte metode kan ikke anvendes på maskiner hvor tastaturet er integrert i maskinen.

Datakrimutvalget finner ikke grunn til å foreslå egne bestemmelser om romavlytting og avlytting av samtaler utendørs i datakrimkapitlet. Det er selve handlingen som her er det vesentlige, og ikke den tekniske fremgangsmåten som benyttes. Slike forhold bør reguleres av teknologinøytrale avlyttingsbestemmelser, som § 145 a nr. 2 i straffeloven.

Uberettiget avlytting i datanettverk er imidlertid datakriminalitet. Ved å kjøre et spesielt program på en datamaskin kan den fange opp trafikk på datanettverket som den er tilknyttet. Eksempelvis er det i trådløse nettverk mulig å fange opp all kommunikasjon mellom basestasjonen og andre maskiner som er tilknyttet samme basestasjon.

Slik avlytting har vist seg å være effektivt i forbindelse med datainnbrudd. Man kan etter et datainnbrudd fange opp nyttetrafikk og tilgangsinformasjon for å gjøre ytterligere datainnbrudd. Således er det nokså vanlig at gjerningspersonen etter han har gjort datainnbrudd på en maskin setter opp et program som avlytter nettverkstrafikken (såkalt sniffer) og lagrer denne til en fil på datamaskinen. På denne måten kan gjerningspersonen fange opp alt som sendes over datanettverket, for eksempel e-post. Siden brukernavn og passord ofte sendes i klartekst over datanettverket vil man også fange opp brukernavn og passord på denne måten, noe som selvsagt er interessant dersom man ønsker å begå nye datainnbrudd. Slike tilgangsdata kan benyttes til å begå nye datainnbrudd, eller man kan bruke dem til å bytte til seg

ytterligere tilgangsdata som beskrevet i avsnittet om passordinnbrudd.

Når det gjelder avlytting av data under kommunikasjon, finner Datakrimutvalget det naturlig at dette reguleres av datakrimkapitlet. Dette gjelder enten dataene er i form av tekst, lyd eller bilder (inkludert bevegelige bilder). Dette innebærer at også uberettiget nedtak av radio- og fjernsynssendinger må karakteriseres som avlytting. Det samme gjelder avlytting av telefonsamtaler uavhengig av hvilken teknologi som benyttes.

Noen tilfeller er av en litt spesiell art. Dette gjelder avlytting i form av stråling. Stråling fra en dataskjerm eller et display på en mobiltelefon kan gi grunnlag for rekonstruksjon av skjermbildet ved tekniske hjelpemidler. Det vises til Sunde 2006 «Lov og rett i cyberspace» side 136-137.

### 3.4.7 Kryptering, dekryptering og passordknekking

Kryptering er mye benyttet som en sikkerhetsmekanisme. Ved kryptering blir en datamengde (klarteksten) forvandlet til en annen datamengde (kryptoteksten) ved hjelp av en kryptoalgoritme og en nøkkel. Kryptoteksten gir ingen mening, og kan bare forvandles tilbake til klarteksten ved hjelp av den samme kryptoalgoritmen og den samme eller en korresponderende nøkkel. Nøkkel er i denne sammenheng en datamengde som fungerer som inngangsdata i kryptoalgoritmen. Nøkkelen er som regel vesentlig kortere enn selve teksten. Et passord er et eksempel på en kryptonøkkel, men det er også kryptonøkler som bare er representert ved en digitalt lagret datamengde uten noe passord. Det bemerkes at bruken av ordet tekst i denne sammenheng ikke må misforstås. Kryptering kan benyttes på en hvilken som helst datamengde slik som tekst, bilder, film, fjernsynssendinger, musikk og annet.

Det skilles mellom symmetrisk og asymmetrisk kryptering. Ved symmetrisk kryptering er nøkkelen for kryptering og dekryptering den samme. Ved asymmetrisk kryptering er det to forskjellige nøkler: En privat nøkkel og en offentlig nøkkel. Asymmetrisk kryptering er meget praktisk for kryptering av meldinger som sendes elektronisk. Skal man sende en kryptert melding, foretar avsenderen kryptering med mottakerens offentlige nøkkel, og mottakeren dekrypterer med sin private nøkkel.

Teorien ved kryptering er at bare den som kjenner nøkkelen skal kunne åpne kryptoteksten. Likevel kan det tenkes måter der uvedkommende klarer å åpne krypterte data. For det første kan det tenkes at kryptoalgoritmen som benyttes inneholder svakheter. I slike tilfeller kan det ved å analysere kryptoalgoritmen og/eller utføre statistisk analyse på kryptoteksten være mulig å frembringe klarteksten uten å kjenne til nøkkelen overhodet. Videre kan det tenkes at uvedkommende på samme måte som brukernavn/passord (se kapittel 3.4.1) har fått tak i kryptonøkkelen. Dersom kryptoalgoritmen er kjent, kan nøkkelen benyttes til å dekryptere datainnholdet.

Dersom en angriper verken har nøkkel eller mulighet for å knekke krypteringen ved kryptoanalyse, gjenstår bare en mulighet: gjette nøkkelen. Dette trenger ikke være umulig om man tar en datamaskin til hjelp. Man kan kort og godt programmere en datamaskin til å prøve ut forskjellige passord og se om den finner ett som gir fornuftig resultat. Et slikt program kan bruke forskjellige strategier. En mulig strategi er rett og slett å prøve alle muligheter. En slik strategi kalles «bruteforce». Hvis nøkkelen er et passord på fem tegn går denne strategien ut på å starte med «aaaaa», deretter prøve «aaaab», «aaaac», «aaaad» og så videre. Etter en tid med prøving og feiling vil man nødvendigvis før eller siden finne det riktige svaret. Hvor lang tid det tar avhenger av lengden på nøkkelen. Med et passord på fem bokstaver vil en vanlig datamaskin vanligvis finne det rette svare i løpet av noen timer. Med et passord på åtte bokstaver kan det derimot ta titalls år, og i tilfeller med lengre nøkler kan tiden for å søke gjennom hele nøkkelrommet være lenger enn solsystemets levetid.

En annen mulig strategi er å basere søket etter korrekte nøkler på kjente ord og uttrykk. Hvis man for eksempel tror at passordet er et ord som finnes i norsk, reduserer dette problemet til å prøve alle ord som finnes i en ordliste, noe som på dagens datamaskiner kan gjennomføres på kort tid. Det er denne siste strategien som vanligvis benyttes ved passordknekking.

Mange datasystemer lagrer brukernes passord som en data beregnet ved en enveisfunksjon (hash). Det er ikke mulig å komme direkte fra hashen tilbake til passordet, men dette er heller ikke nødvendig for datasystemets autentiseringsprosedyre, siden denne bare lager en hash av det inntastede passordet og sammenligner denne med hashen som er lagret. Dette systemet ble tidligere ansett som så sikkert at passordfilen på de fleste systemer var lagret slik at den var åpent tilgjengelig for alle brukerne på systemet. Man regnet med at systemet med enveisfunksjon gjorde det umulig å få tak i passordene. Dette viste seg imidlertid å være feil. Ved hjelp av spesielle programmer, passordknekkere, ble det i stor stil foretatt knekking av

passord ved hjelp av ordlistemetoden. Dette ble særlig populært ved utdanningsinstitusjoner hvor det er datasystemer med flere titalls tusen brukere. Hvis man har en passordfil med tjue tusen brukere er det sannsynlig at minst en av dem har et passord som står i en ordliste.

Selv om mange datasystemer i dag lagrer passordfilen på en slik måte at det bare er systembrukeren som kan lese passordhashen, er passordknekking fortsatt en aktuell metode. En av årsakene til dette er at brukere ofte benytter det samme passordet på forskjellige datamaskiner hvor de har tilgang. Å knekke en brukers passord kan derfor gi tilgang på mange forskjellige datamaskiner, muligens også maskiner hvor man ikke hadde mulighet til å skaffe seg tilgang på annen måte.

Kryptering vil være særlig aktuelt ved lagring eller forsendelse av sensitiv informasjon. Dette kan gjelde informasjon som er undergitt taushetsplikt, for eksempel informasjon som er undergitt taushetsplikt for leger eller advokater. Andre eksempler er lagring av informasjon om kunders kredittkort og passord hos nettbutikker, og lagring av personopplysninger hos forvaltningen. Anvendelse av kryptering sikrer dataenes konfidensialitet.

En form for kryptering som har vært vanlig i mange år ved netthandel er den såkalte SSL-protokollen. Denne benyttes ved overføring av betalingsdata (kredittkortdetaljer m.v.) fra kunden til nettbutikken. Krypteringsløsningen er innebygget i kundens nettleser. De aller fleste som har handlet på nettet har stiftet bekjentskap med denne teknologien, men for manges vedkommende sikkert uten å legge merke til det.

Det er åpenbart at det er et mål for kriminelle å skaffe seg kjennskap til innholdet av krypterte data.

### 3.4.8 Selvspredende programmer

Ovenfor er forskjellige typer programmer som kan være skadelige omhandlet; exploits, trojanere, rootkit, skannere, sniffere og passordknekkere. Disse programmene har til felles at de for å volde skade på en datamaskin må være kjørt av en gjerningsperson mot den aktuelle målmaskinen. Etter omstendighetene kan det ut fra disse programmenes funksjon og virkemåte neppe være tvilsomt hva intensjonen til gjerningspersonen har vært. Programmene rammer etter sin art bare et begrenset utvalg datamaskiner, nemlig det utvalget som gjerningspersonen har bestemt. Skadepotensialet til disse programmene er derfor begrenset til det mål gjerningspersonen velger seg ut når han kjører dem.

Selvspredende programmer skiller seg vesentlig fra programmer som er behandlet over. Selvspredende dataprogrammer er programmer som ved å utnytte de metoder som er beskrevet tidligere i dette kapitlet, kopierer seg selv og derved sprer seg selv videre til andre datamaskiner. Ved å spre seg selv til stadig nye datamaskiner, kan slike programmer oppnå en rask spredning til svært mange datamaskiner, og potensielt utrette skade på disse. Skaden kan bestå i konkrete funksjoner som er lagt inn i programmet, for eksempel sletting av filer. Men selv om programmet ikke er programmert til å utføre en bestemt skade, så representerer det at programmet kopierer seg selv til andre datamaskiner en skade i seg selv. Siden innehaveren av datamaskinen som er infisert ikke kan kjenne alle egenskapene programmet har, må maskinen i utgangspunktet behandles som om den var utsatt for datainnbrudd, jf. diskusjonen under kapittel 3.4.3.

Selvspredende dataprogrammer finnes i mange forskjellige former og har tradisjonelt fått forskjellig navn alt etter formen. Virus har tradisjonelt vært ansett som et program som ved hjelp av å hekte seg selv på et annet dataprogram blir aktivert når det andre dataprogrammet blir kjørt. Denne formen for virus dukket opp allerede på 1980-tallet, og var velkjent både på datamaskinplattformen og på andre plattformer som for eksempel Commodore og Amiga. Når slike virus blir aktivert, blir kopier av viruset lagt til forskjellige eksekverbare programmer som allerede finnes på datamaskinen. Mange tidlige virus fokuserte spesielt på programmer som var lagret på diskett, siden dette var måten de kunne spre seg til andre datamaskiner. (På denne tiden var det uvanlig at datamaskiner var tilknyttet nettverk.)

I de senere år har imidlertid virusbegrepet tildels fått en annen betydning. Begrepet brukes i dag mest om selvspredende programvare som bruker e-post som spredningsmekanisme. Viruset kopierer da seg selv til et e-postvedlegg. Denne e-posten sendes så til alle e-postadresser som viruset kjenner til, vanligvis alle e-postadresser som den rettmessige brukeren av den infiserte maskinen regelmessig kommuniserer med. For å få mottakeren til å åpne e-posten og kjøre virusprogrammet, benyttes metoder som minner om metoder som vanligvis benyttes for å få en mottaker til å kjøre en trojaner, jf. kapittel 3.4.1. Jo flere mottakere viruset klarer å lure til å åpne vedlegget, jo mer vil viruset bli spredt. Således er kanskje det best kjente eksemplet på e-postvirus viruset *ILOVEYOU*, som

fikk enorm spredning i april-mai 2000. Dette viruset kamuflerte seg selv som et kjærlighetsbrev som vedlegg til e-post, en metode for sosial manipulering som viste seg meget effektiv for å spre viruset mest mulig. ILOVEYOU-viruset skal ha infisert minst 45 millioner datamaskiner over hele verden.

I litteraturen omtales selvspredende programmer som sprer seg selv via datanettverk, oftest som ormer. En orm er et program som gjør datainnbrudd på andre datamaskiner ved hjelp av metodene beskrevet under 3.4.1 og 3.4.2. De fleste ormer utnytter en bestemt sårbarhet. Så snart ormen er startet på en maskin starter den breddeskanning etter andre datamaskiner som har sårbarheten ormen utnytter, jamfør beskrivelsen i 3.4.2. Når den har funnet en maskin som har denne sårbarheten, utnyttes denne med en exploit som er innebygget i ormen. Dette gir ormen tilgang til å kjøre programmer på den andre datamaskinen. Dette utnytter ormen til å kopiere seg selv og starte seg selv på den nye datamaskinen. Dermed er også denne maskinen infisert av ormen og prosessen starter på nytt. På denne måten kan en orm spre seg til et meget stort antall maskiner på relativt kort tid. Spredningstakten avhenger av flere forhold, hvor det ser ut til at andelen av datamaskiner på internett som har den bestemte sårbarheten er det viktigste parameter.

Det beste eksempel på rask spredningstakt av en orm finnes kanskje ved ormen «Slammer». Denne ormen startet spredningen den 25. januar 2003 klokken 06:30 norsk tid. I løpet av det første minuttet den kjørte, doblet populasjonen seg hvert 8. sekund. Etter tre minutter nådde ormen den høyeste totale skan-raten, på dette tidspunkt skannet ormen totalt over 55 millioner IP-adresser per sekund. Etter bare ti minutter nådde ormen sin maksimale populasjon; over 75000 datamaskiner var da infisert. Slammer-ormen utnyttet en sårbarhet i programmet Microsoft SQL-server. Dette er et program som bare brukes på servere og er relativt uvanlig. Dersom ormen istedet hadde utnyttet en sårbarhet på vanlige brukermaskiner, er det sannsynlig at populasjonen hadde blitt langt større. Heldigvis inneholdt ikke Slammer destruktiv programkode ut over selve spredningen, men den raske spredningstakten beviste at det er mulig å lage en orm som gjør stor skade på flere millioner datamaskiner over hele internett. Med så rask spredningstakt som Slammer hadde er det nemlig ikke mulig å iverksette effektive mottiltak for å hindre spredningen. Hvis noen kjenner til en nyoppdaget sårbarhet, vil det være mulig for dem å lage en orm som sprer seg til flere millioner datamaskiner over hele internett i løpet av 10-15 minutter. Ormen kan så slette alle data på alle disse datamaskinene, eller starte massive tjenestenektangrep som vil føre til at infrastrukturen internett er bygget på bryter sammen. En slik potensiell orm kalles en Warhol-orm, etter Andy Warhols utsagn «In the future, everyone will have 15 minutes of fame».

Det skulle derfor være klart at selvspredende dataprogrammer kan være meget farlige, og har betydelig skadepotensial. Skaden oppstår idet programmet starter å spre seg selv. Etter at dette tidspunktet er passert er det ikke lenger mulig for opphavsmannen til programmet å kontrollere det. Programmet lever etter dette så og si sitt eget liv. Det finnes eksempler på at selvspredende programmer har sluppet ut uten bevisste handlinger fra opphavsmannen. Dersom man eksperimenterer med selvspredende programmer kan det fort skje at programmet «slipper ut», og starter å spre seg selv utenfor opphavsmannens kontroll. Hvorvidt programmet er sluppet ut bevisst eller ubevisst har dog mindre betydning for konsekvensene av selvspredende kode, siden den samme skaden vil skje uansett.

De juridiske sider ved denne typen programmer behandles i kapittel 5.7.6.

### 3.4.9 Tjenestenektangrep

Tjenestenektangrep (eller DoS-angrep etter den engelske betegnelse «Denial-of-Service») er en angrepsform som utelukkende rammer et datasystems tilgjengelighet. Ved denne angrepsformen angripes et datasystem på en slik måte at det ikke kan brukes slik det var ment – for eksempel at det ikke er mulig å bruke internett fra datasystemet.

Tjenestenektangrep kan deles inn i to hovedkategorier; tjenestenekt som utnytter sårbarheter og tjenestenekt ved overbelastning. Førstnevnte minner om datainnbrudd ved å utnytte sårbarheter i datasystemer. Men isteden for at målet er å trenge seg inn og skaffe seg uberettiget adgang til datasystemet, er målet bare at det skal oppstå en situasjon der datasystemet ikke kan benyttes som normalt. Et klassisk eksempel på dette er «Ping of Death». Dette angrepet var mulig mot tidligere versjoner av Windows-operativsystemet, fordi disse versjonene ikke sjekket lengden på innkommende datatrafikk i ICMP-protokollen som benyttes av nettverksverktøyet Ping. Hvis det kom inn datapakker som var større enn den tillatte størrelsen, ville operativsystemet låse seg eller eventuelt krasje. Med programmet Ping of Death, som nettopp laget slike store pakker, var det derfor mulig for hvem som helst å få andres datamaskiner til å kra-

sje ved å kjøre dette programmet mot dem. Dersom slike sårbarheter er kjent, er det mulig for innehavere av datasystemer å forhindre at dette skjer. Det vises til drøftelsen under avsnittet om sårbarhetsinnbrudd i kapittel 3.4.1.

Tjenestenekt ved overbelastning er betydelig vanskeligere å forhindre. Den vanligste formen for slik tjenestenekt er at man forhindrer et datasystem i å kommunisere med internett ved å sende så store mengder med meningsløse data mot systemet at internettforbindelsen blir fylt opp. I slike tilfeller vil det være svært vanskelig eller umulig å gjennomføre fornuftig kommunikasjon med målsystemet. For å gjennomføre et slikt angrep kan det være nødvendig å gå gjennom en forberedelsesprosess. Man kan nemlig vanligvis ikke produsere store nok datamengder til å blokkere et datasystem fra en enkelt maskin. Det er nødvendig å ha kontroll over mange maskiner for å gjennomføre et koordinert angrep. Det er vanlig at man bruker teknikkene som er beskrevet tidligere i dette kapitlet for å gjennomføre datainnbrudd på et større antall datamaskiner. På disse maskinene installerer man så et dataprogram, kalt agent, som fjernstyres til å sende store datamengder mot en bestemt adresse. Angrepene kan startes og stoppes ved å sende kommandoer til alle agentene om hvilke adresser de skal angripe. Hvor effektivt det resulterende angrepet blir avhenger av hvor mange agenter man fjernstyrer, samt hvor mye data hver agent klarer å sende. Sistnevnte avhenger både av maskinkapasitet på agentmaskinen, og størrelse på internettforbindelsen.

Tjenestenektangrep ved overbelastning av internettlinjen er i praksis svært vanskelig å forhindre eller stoppe. Årsaken er både at avsenderadressen på datatrafikken kan være forfalsket, og at det er svært mange mellomledd som må undersøkes for å spore angrepet tilbake til opprinnelsen. Med dagens teknologi er det i praksis nærmest utelukket å finne ut hvem som står bak et angrep ved å spore angrepet. I de fleste tilfeller er man derfor henvist til å stoppe angrepet ved å forsøke å filtrere angrepstrafikken hos internettleverandørene som leverer forbindelsen til datasystemet som blir angrepet. Det har i de senere år forekommet flere tilfeller av utpresning hvor en gjerningsperson har startet tjenestenektangrep mot virksomheter som er avhengig av sin internettforbindelse og deretter krevd betaling for å stoppe angrepet. Ifølge rapporter fra det føderale amerikanske politiet FBI velger mange å betale utpresserne heller enn å gjøre forsøk på å finne ut hvem som står bak og stoppe angrepene, fordi man vet hvor vanskelig dette er.

Det er også mulig å fremkalle en tjenestenektsituasjon ved å kjøre programmer på en datamaskin som spiser opp alle ressursene på maskinen. En måte å konsumere ekstra mye ressurser på er å lage et program som starter seg selv mange ganger. Et slikt program kalles av og til en bakterie.

Ved tjenestenektangrep er det mulig å stoppe datasystemer som kan være av vital betydning. Det er også mulig å forårsake store økonomiske tap, for eksempel ved at en nettbutikk med stor omsetning settes ut av drift over lengre tid. Datakrimutvalget anser derfor denne typen angrep som svært alvorlig. Nærmere omtale av de juridiske sidene finnes i kapittel 5.6.4.

## 3.5 Gamle trusler i moderne utgave

Den store utviklingen i datateknologien og konnektiviteten blant annet via internett, fører til at også de kriminelle følger etter og tar i bruk datatekniske hjelpemidler for å begå tradisjonell kriminalitet. Denne kriminaliteten begås der folk gjør sine transaksjoner, for eksempel ved netthandel og betalingstransaksjoner. Verken vanlige fysiske butikker eller nettbutikker får være i fred for anslag fra kriminelle.

Pengefalsk er en gammel form for kriminalitet. Falske penger kan lett fremstilles ved hjelp av datautstyr. Pengesedler skannes for eksempel inn på en datamaskin, og falske pengesedler kan skrives ut ved hjelp av moderne fargeskrivere. Denne formen for kriminalitet er det imidlertid ikke naturlig å betegne som datakriminalitet, og den behandles ikke nærmere i utvalgets innstilling. Det samme gjelder fysisk tyveri av datamaskiner og fysisk skadeverk på datamaskiner. Dette må normalt anses som tradisjonelle former for tyveri og skadeverk.

Det vil ofte ikke være noe skarpt skille mellom gammel kriminalitet på nye måter, som er behandlet i dette kapitlet, og moderne former for datakriminalitet som er behandlet i de foregående kapitler. Sondringen har imidlertid ikke noen rettslig betydning. Kriminalitet i elektroniske miljøer er blitt gitt en del nye karateristikker. Disse begrepene, som man i stor utstrekning kan finne i avisene hver dag, har ikke noe entydig definert innhold. Når de likevel er benyttet i denne fremstillingen, er det fordi de kan være nyttige ved de assosiasjoner de vil vekke.

### 3.5.1 Omsetning av tyvegods

Salg av tyvegods og andre gjenstander selgeren ikke har lovlig adgang til, er vanlige tradisjonelle

former for kriminalitet. Nettauksjoner og annonser på tekst-tv er nye kanaler som tas i bruk for dette formål. Her kan selgerne operere diskret og anonymt overfor et stort publikum av potensielle kjøpere. Omsetning av brukte gjenstander er vanlig på slike markedsplasser, og det er derfor ikke like lett å fatte mistanke som hvis salget foregår i en mørk bakgate. Selgeren kan etter omstendighetene straffes for tyveri eller heleri. Er kjøperen klar over at han kjøper tyvegods eller handler uaktsomt, kan han straffes for heleri. Utvalget bemerker at det ikke i seg selv kan være uaktsomt å handle for eksempel på nettauksjon, men prisen på varen og andre omstendigheter kan tilsi at det foreligger straffbar uaktsomhet, jf. straffeloven § 317 syvende ledd (uaktsomt heleri). Utvalget har ikke gått nærmere inn på disse problemstillingene i lovforslaget.

### 3.5.2 Levering av gjenstander som ikke oppfyller kjøpers rimelige forventninger ved netthandel

Ved netthandel og nettauksjoner forekommer det ikke sjelden at den varen kunden får tilsendt – og som han som regel ikke får se før etter at han har betalt – ikke svarer til bestillingen. Det har hendt at en kjøper har bestilt for eksempel en datamaskin, men i stedet ligger det en murstein i pakken. Andre eksempler kan være at datamaskinen er mye dårligere enn de spesifikasjonene som ble angitt på nettstedet som kunden bestilte fra. Leveransen kan også bestå i piratkopier av merkevarer eller brukte varer istedenfor nye. Det kan endog hende at levering av varen totalt uteblir. De tilfeller som her er nevnt, må normalt anses som bedragerier, jf. straffeloven § 270 første ledd nr. 1, og de fordrer ingen særskilte bestemmelser i datakrimkapitlet. Det må imidlertid sondres mellom kjøpsrettslige mangler og bedragerier. Det skal betydelig mer til for at det skal foreligge et bedrageri enn en kjøpsrettslig mangel som gir grunnlag for sivilrettslige beføyelser. For øvrig vises det til forrige kapittel om omsetning av tyvegods.

### 3.5.3 Bedragerier m.v. på internett

Mange kjente og gamle konsepter for bedrageri benyttes over internett. For eksempel distribueres såkalte «Nigeriabrev» ved e-post, i tillegg til ved papirbasert post.

En tilsvarende og velkjent form for bedrageri eller bedrageriforsøk, er at man mottar melding om å ha vunnet en stor gevinst i et pengelotteri (hvor man ikke en gang har kjøpt lodd). For å få utbetalt gevinsten, må man oppgi kredittkortnummeret for trekk av et mindre administrasjonsgebyr. De som gjør dette ser imidlertid ikke noe til gevinsten. Den kontoinformasjon som er avgitt kan også misbrukes.

Det finnes utallige former for slik ulovlig virksomhet. Svindlerne benytter seg både av falske nettsider og e-post hvor spredningsmetoden ofte er spam (se kapittel 3.6). De tar også direkte kontakt med potensielle ofre via kontaktfora på internett. Internett gir store muligheter for å operere internasjonalt og under falsk identitet. Ut over bruken av spam, skiller ikke fremgangsmåtene seg fra det man er vant til fra tidligere. Det er neppe nødvendig å foreslå nye bestemmelser annet enn for spam, for å ha hjemmel for straff i slike tilfeller. På grunn av sakenes internasjonale karakter kan det uansett være vanskelig å få gjennomført strafforfølgning rent praktisk.

### 3.5.4 Anslag mot minibanker

Fysisk anslag mot minibanker har forekommet. Dette anses som tradisjonelle tyverier og skadeverk og behandles ikke her.

Minibankautomater kan også være gjenstand for anslag på mange andre måter. Det kan bli gjort uttak med falske, tapte eller stjålne bank- eller kredittkort. Uttakene kan også bli gjort i større utstrekning enn kortinnehaveren har rett til, for eksempel fordi det ikke er penger til å dekke uttaket på et debetkort. For de juridiske implikasjonene av dette vises det til kapittel 5.8.

Et anslag mot en minibank kan også ha et indirekte formål. Kriminelle kan feste såkalte skimmere til en minibankautomat slik at dataene på kundenes kort blir kopiert uten at kunden merker dette. Skimmeren sitter i en falsk front som monteres utenpå minibanken der kortet settes inn. Dataene som er kopiert i skimmeren danner grunnlag for etterfølgende produksjon av falske kort.

Bruk av skimmer er gjerne kombinert med at det er festet et lite videokamera på minibanken som filmer tastaturet. Filmen overføres til en liten bærbar datamaskin i nærheten. På den måten kan gjerningsmannen se hvilken pinkode kunden taster.

Etter dette har gjerningspersonen skaffet seg både pinkoden og kopi av dataene i kortet. Kunden vil på sin side ikke ha merket noe. Dataene og informasjonen kan overføres elektronisk til et produksjonssted som produserer falske kort, og det falske kortet blir ofte benyttet i en annen del av verden kort tid etter at anslaget fant sted.

En annen metode er en såkalt «libanesisk slynge» («Lebanese loop»). Etter denne metoden fester man en anordning, en slynge, til en minibank, som fanger opp kortet slik at det ikke kommer ut av bankautomaten igjen. Når kunden har forlatt stedet, fisker gjerningspersonen ut slyngen som inneholder kortet, og vedkommende har på den måten klart å tilegne seg kortet.

«Venezuelansk skrutrekker» («Venezuelan Screwdriver») er en annen metode. Ved fysisk påvirkning på minibanken hindres registrering av en utbetaling som faktisk har funnet sted. Det kan derved tas ut mer penger på kortet enn det er dekning for.

Bankene arbeider med bedre sikkerhetssystemer for å motvirke slike former for anslag. På den annen side tar også de kriminelle i bruk stadig nye metoder. Den strafferettslige tilnærming til disse formene for anslag er behandlet i kapittel 5.4.3, 5.7.4 og 5.8.

### 3.5.5 Andre måter å fange opp kortinformasjon

Skimming av kort som nevnt ovenfor, skjer oftest på brukerstedet. Det er også mulig å kopiere informasjon om betalingskort og sikkerhetskoder fra den datastrøm som overføres mellom brukersted og kortutsteder (tapping av data under overføring). Dataene kan også kopieres i forbindelse med et innbrudd i en kredittkortdatabase.

### 3.5.6 Falske kort

Ovenfor er det vist til flere muligheter for å skaffe data og informasjon som kan benyttes til å fremstille falske betalingskort. Hva som kreves av et falsk kort, er avhengig av hvilken bruk som er påtenkt. I noen tilfeller kan det produseres nytt plastkort som er påsatt falsk bilde og falsk underskriftsprøve. Dette er nødvendig i situasjoner hvor kortet skal brukes på steder de kontrolleres av mennesker. I andre situasjoner skal kortet brukes i forhold til maskiner, og da er det andre ting som er viktige, nemlig data i magnetstripe og/eller smartkort, ofte kombinert med pinkoder. Noen situasjoner innebærer både maskinell bruk og kontroll fra mennesker, for eksempel betaling med kredittkort på spisesteder som sjekker kortet online. Produksjon og bruk av falske kort er behandlet i kapittel 5.8 og 5.9.

### 3.5.7 Misbruk av kortinformasjon

Ved netthandel er det som regel ikke nødvendig å ha kortet som skal brukes til betalingen fysisk tilgjengelig. Det er tilstrekkelig at man har kortnummeret og kortets utløpsdata. I noen tilfeller er også brukerens navn og adresse nødvendig, avhengig av hvor omfattende selgerens kontrollrutiner er. Ofte kreves i tillegg et verifikasjonsnummer som ligger i CVV-nummeret på kortet (Card Verification Value (CVV)). Disse opplysningene representerer kortet i situasjoner hvor det ikke lar seg presentere rent fysisk, for eksempel ved betalingstransaksjoner over internett. Det betyr at en kriminell kan begå såkalt «kredittkortbedrageri» ved å avgi denne kortinformasjonen som vedkommende har skaffet seg, uten å ha selve kortet i hende.

Sikkerheten blir imidlertid stadig bedre, og nettbutikkene tar etter hvert i bruk sikrere løsninger i samarbeid med kortleverandørene. Dette innebærer blant annet at man benytter ny sikkerhetskode for hver gang kortet brukes (engangspassord) og elektronisk signatur.

### 3.5.8 Andre elektroniske betalingsmidler

I tillegg til debet- og kredittkort er det utviklet en rekke andre tjenester for betaling på internett. Man kan ha midler knyttet til for eksempel en konto hos PayEx, PayPal eller BuyPass. Disse midlene kan benyttes til elektronisk betaling ved belastning av kontoen. Det er ofte mindre beløp som det er praktisk å betale ved slike transaksjoner. I tillegg er det på forsøksstadiet utviklet magnetbrikker og smartkort som inneholder pengebeløp og kan belastes ved avlesning på salgsstedet.

Lov om e-pengeforetak av 13. desember 2002 nr. 74 inneholder rammebetingelser for dem som utsteder betalingsmidler i form av elektroniske penger. Rettslig betyr elektroniske penger en pengeverdi kunden har som fordring mot utstederen, som er lagret på elektronisk medium og som er utstedt etter mottak av midler fra kunden.

Også konti av denne typen kan være gjenstand for misbruk, og representasjonene de eventuelt er knyttet til kan være gjenstand for forfalskning eller fremstilling av falske representasjonsenheter. Det vises til kapittel 5.8 og 5.9.

### 3.5.9 Reisekort, elektroniske billetter m.v.

Rettigheter til å ta ut tjenester knyttes ofte til elektroniske reisekort, elektroniske billetter, bombrikker, ringekort, kodekort for betalings-tv osv. Adgangskort fremstilles elektronisk og trer iste-

denfor nøkler til tradisjonelle låser. Ofte benyttes adgangskortene sammen med brukers pinkode.

Kriminelle kan fremstille falske eksemplarer av alle disse representasjonene. Representasjonene kan også bli stjålet og misbrukes av tyven. Det vises til behandlingen i kapittel 5.8 og 5.9.

### 3.5.10 Elektronisk prising

I butikker hentes nå nesten all informasjon om vareidentitet og varepris fra strekkoder som avleses maskinelt. Falske strekkoder, som for eksempel limes over de ekte strekkodene, kan derved påvirke den prisen kunden betaler for varen. Det vises her til kapittel 5.8 og 5.9.

### 3.5.11 Bistand til å skaffe ulovlig adgang til datasystemer

*Hjelp fra innsiden*

For kriminelle som ønsker å skaffe seg tilgang til et datasystem, vil det være nærliggende å søke hjelp hos personer som besitter nødvendige tilgangsdata som for eksempel brukernavn og passord. Det er heller ikke utenkelig at kriminelle bestikker ansatte for å få slike opplysninger. Videre kan det tenkes at ansatte eller andre som besitter slike data, trues eller presses til å gi kriminelle opplysningene. Misfornøyde eller tidligere ansatte kan også tenkes å ha et hevnmotiv overfor vedkommende arbeidsgiver. Personer med tilknytning til bedriften kan også hjelpe kriminelle til å komme inn i lokalene for å få fysisk tilgang til datasystemene.

Etter omstendighetene vil hjelperen på innsiden kunne holdes strafferettslig ansvarlig som medvirker til det lovbruddet som den kriminelle hovedmann begår. Det kan også være aktuelt med straff for økonomisk utroskap, jf. straffeloven § 275, og eventuelt for bestikkelse, jf. straffeloven § 276a og 276b.

*Sosial manipulering*

En fremgangsmåte som særlig er kjent fra utlandet, er at kriminelle søker å forlede ansatte til å gi fra seg opplysninger om tilgangsdata. Dette er betegnet som «Social Engineering», og kan utvikles til en hel vitenskap. I boken «The Art of Deception» gir Kevin D. Mitnick en tankevekkende oversikt fylt med eksempler på hvordan dette kan gjøres.

Et typisk eksempel kan være at en ansatt får en telefon fra for eksempel Tom i «brukerstøtte». Han høres meget troverdig ut og opplyser at det har vært et datakrasj i bedriften (noe som brukeren for øvrig selv har kunnet konstatere, men uvitende om at det er Tom selv som nettopp har forårsaket krasjet for å gjøre henvendelsen troverdig). Han sier at han trenger den ansattes brukernavn og passord for å gjenopprette dataene. Brukeren, som er stresset for ikke å bli ferdig med en presserende jobb og dessuten nervøs for datatap, oppgir i farten brukernavnet og passordet. Og straks er forbryteren inne i systemet.

Et annet eksempel er at det dukker opp en person i kjeledress som sier han skal bytte et modem. Oppdraget påstår han å ha fått av systemadministrator, som han på forhånd vet ikke er til stede når han kommer. Han virker troverdig, blant annet fordi han kjører en firmabil som tilhører en kjent dataleverandør og også har denne leverandørens logo på kjeledressen. De ansatte slipper ham inn i datarommet og lar ham bli igjen alene der. Han har da tilgang til datasystemene og kan for eksempel legge inn en «bakdør» slik at han har fremtidig tilgang til systemet fra utsiden.

### 3.5.12 Misbruk av identitet

*Innledning*

Misbruk av identitet innebærer at noen på en eller annen måte urettmessig benytter en annens identitet. Ofte kalles dette «identitetstyveri». Det kan skilles mellom økonomisk identitetstyveri og annet misbruk av identitet.

Vanlige eksempler på økonomisk identitetstyveri er at man benytter falsk legitimasjon i skranken i banken i forbindelse med uttak fra en annens konto, eller urettmessig belastning av en annens konto ved handel på internett. Det samme gjelder ved uttak av penger fra en minibank ved hjelp av stjålet eller falskt bankkort. Identitetstyverier består her rent konkret i misbruket av pinkoden, som er en opplysning som nettopp skal verifisere at det er rette innehaver av kortet som benytter det.

Det kan også kalles identitetstyveri dersom en person sender ut e-post, tekstmeldinger, post eller lignende som utgir seg for å komme fra en annen enn avsenderen. Handlingen kan være økonomisk motivert eller skyldes andre grunner. Formålet kan for eksempel være å komme i kontakt med barn eller ungdom med tanke på senere seksuell omgang. Atter en annen variant er at det opprettes en webside på internett som ledd i phishing, se neste avsnitt. Selve metoden er basert på at det kriminelle foretaket søkes forvekslet med et lovlig, dvs. en integritetskrenkelse.

Noen ganger vil formålet med identitetstyveriet være å overta en bestemt persons identitet – for eksempel for å benytte vedkommendes bankkort eller gode omdømme. Andre ganger vil formålet være å skjule sin egen identitet, og det vil da være tilfeldig hvilke identiteter som misbrukes.

Både enkeltpersoner og juridiske personer kan bli utsatt for identitetstyveri. Identitetstyveriet kan også knytte seg til et alias, for eksempel et kallenavn som benyttes på en chattekanal, eller en e-postadresse som ikke er umiddelbart identifiserbar i forhold til noen person.

Et eksempel på et identitetstyveri er at det opprettes en webside på internett som utgir seg for å tilhøre en bedrift, men som ikke tilhører denne bedriften. Dette kan for eksempel være en falsk nettside som utgir seg for å tilhøre en kjent bank. Når kunder forledes til denne og oppgir brukernavn og passord m.v., kan denne informasjonen misbrukes av kriminelle i forhold til den rette nettbanken.

*Phishing*

I de senere årene er det opptått en ny form for svindel på internett som populært kalles «phishing», som på norsk gjerne kan betegnes som «fisking». Metoden baserer seg på identitetstyveri. Den vanligste formen går ut på å sende e-post til et stort antall mottakere ved bruk av spamteknologi (se kapittel 3.6). E-posten utgir seg for å komme fra en velrenommert kilde, for eksempel en bank eller et kredittkortselskap. Det «informeres» ofte om at det har oppstått en feil i bankens datasystem, og at kunden må verifisere sine kontoopplysninger for at kontoen fortsatt skal være operativ. E-posten inneholder gjerne bankens logo, og kunden blir bedt om å gå til bankens nettside for å verifisere kontoopplysningene. E-posten inneholder tilsynelatende en lenke til bankens nettside.

Når kunden klikker på lenken, kommer han til en nettside som er til forveksling lik bankens nettside. Nettsiden er imidlertid falsk – det vil si at den tilhører dem som står bak «phishinghandlingen». Kunden blir bedt om å logge seg inn på nettsiden ved hjelp av sitt brukernavn og passord (alle brukernavn og passord aksepteres naturligvis), og kommer deretter til et skjema han må fylle ut. Der skal han oppgi kontonummer, sikkerhetskoder, personopplysninger, pinkode m.v. for å verifisere kontoen. De innsendte opplysningene kan deretter danne grunnlag for forskjellige former for misbruk, herunder produksjon av falske betalingskort, eller til å tømme kundens konto ved kontantuttak eller ved urettmessige belastninger. Informasjonen kan også omsettes i det kriminelle miljøet (informasjonsheleri).

En grundig og innsiktsfull oversikt over phishing er gitt av Lininger og Vines i boken «Phishing. Cutting the Identity Theft Line».

*Falsk avsenderangivelse og falske nettsider*

Også bruk av falsk avsenderangivelse på elektroniske meldinger og falske nettsider kan representere identitetstyveri. En variant er at gjerningspersonen sender en e-post eller tekstmelding som fremstår som sendt fra en annen enn den virkelige avsender. Typisk vil «phishing-mail» som tidligere nevnt fremstå som om den er sendt fra en bank eller et kredittkortselskap. En tekstmelding kan fremstå som om den er sendt fra en venn. Det finnes også metoder for å forfalske en nettside, slik at den fremstår som om den har en annen internettadresse (URL) enn den virkelige. Ved phishing er det for eksempel viktig at kunden tror at han befinner seg på bankens nettside når han «logger inn» og «verifiserer» sine kontoopplysninger. Det fører for langt å komme nærmere inn på alle disse teknikkene her.

### 3.5.13 Angrep mot navnetjenersystemet

Internett er organisert i et navnetjenersystem (Domaine Name System) der hver nettside har sitt domenenavn. For å finne en side må man skrive domenenavnet inn i adressefeltet på nettleseren. De såkalte navnetjenerne «oversetter» domenenavnet til den IP-adressen hvor vedkommende side er lokalisert. E-postadresser er også knyttet til domenenavn, og identifikasjonen fungerer her på samme måte.

Ved å sørge for at trafikken til for eksempel en nettbutikk blir dirigert til en falsk nettbutikk av navnetjenerne, gis kriminelle mulighet til å få påloggings- og betalingsdata. I tillegg kan den falske nettbutikken overta omsetningen fra den ekte. Ved å skaffe seg ulovlig tilgang til en navnetjener og endre informasjonsfilene kan man overta kontrollen med et domene. Det finnes også noen andre varianter av angrep mot teknisk utstyr som kan gi denne virkningen. Slike angrep er også kalt «pharming». Handlingene vil etter utvalgets forslag kunne straffes som ulovlig tilgang til datasystem og som datamodifikasjon, se kapittel 5.6.2 og kapittel 5.6.3.

Angrep på navnetjenersystemet rammer internetts infrastruktur fordi det medfører at brukere som oppsøker adressen til et bestemt nettsted i stedet blir sendt til en annen nettside. Dette åpner for

misbruk og svindel som brukeren vanskelig kan beskytte seg mot.

En annen metode er å sende inn en falsk endringsmelding via en registrar. Det hender ofte at en nettside bytter ISP-leverandør, og oppdatering i navnetjenersystemet må skje i denne forbindelse. Ved hjelp av falske meldinger kan det være mulig å overta kontrollen med et domene. Slike forhold må bedømmes som bedrageri eller forsøk på bedrageri, og krever ingen lovendring.

Brukere kan også ledes til falske nettsteder ved at en angriper endrer lokale filer på den enkelte brukers datasystem. Dette kan skje gjennom ulovlig inntrengning, og det må også etter utvalgets lovforslag vurderes som uberettiget tilgang til datasystem og datamodifikasjon, jf. kapittel 5.6.2 og 5.6.3.

### 3.5.14 Uønskede kontakter via internett

Internett benyttes i stor grad til kommunikasjon. Folk som ikke kjenner hverandre fra tidligere, kan komme i kontakt. Dette skjer i en rekke kanaler, for eksempel i egne internettsamfunn, åpne og lukkede chattekanaler, nettbaserte spill osv. Mulighetene er utallige. I et moderne samfunn kan det skje en betydelig nettverksbygging over internett, og dette er i utgangspunktet positivt. Imidlertid er ikke alle kontakter positive.

Kommunikasjon over internett gir ubegrensede muligheter til å opptre under falsk identitet. En som utgir seg for å være en 13 år gammel jente, kan i virkeligheten godt være en mann på 60 år. Dette innebærer blant annet at det kan skje en kontaktbygging over internett hvor voksne forbereder møter for å begå seksuelle overgrep mot mindreårige. Den mindreårige tror kanskje at hun eller han chatter med en ungdom som er kjent som idrettsstjerne, mens de i virkeligheten har kontakt med en voksen potensiell overgriper. Vedkommende kan søke å avtale møter med den mindreårige under falske foregivender, for eksempel med tanke på å begå seksuelle overgrep. I denne anledning har Justisdepartementet foreslått regler om såkalt «grooming», jf. Ot.prp. nr. 18 (2006-2007). Groomingbestemmelsene er behandlet som en separat sak i forhold til datakrimbestemmelsene.

Man kan også få kontakter over internett som senere viser seg å bli plagsomme. Det kommer blant annet e-post av trakasserende art. Dette er internasjonalt kjent under betegnelsen «Cyberstalking». Utvalget har foreslått en endring i nåværende straffelov § 390 a i denne anledning, og det vises til kapittel 5.14.

### 3.5.15 Krenkelser av opphavsrett

Åndsverkloven § 2 gir som hovedregel den som har opphavsretten til et åndsverk enerett til å tilgjengeliggjøre verket for allmennheten eller til å fremstille eksemplarer av åndsverket. Opphavsretten kan overdras. Det er vanlig at opphavsretten til bøker, musikk osv. er overdratt til forlag, plateselskaper og lignende. Det er derfor i stor grad kapitalsterke medieselskaper som innehar opphavsrettigheter i dag.

Vern av opphavsrett og nærstående rettigheter er forøvrig regulert av datakrimkonvensjonen artikkel 10. I Datakrimutvalgets delutredning I (NOU 2003: 27), er forholdet til denne bestemmelsen behandlet på sidene 26-30. Det ble konkludert med at det ikke var behov for endringer i norsk rett for å implementere artikkel 10.

Utgangspunktet for det meste av musikk og film er at det er åndsverk som er vernet av åndsverkloven. Denne gir opphavsmannen eller den opphavsretten er overdratt til en enerett til å fremstille eksemplarer og gjøre det tilgjengelig for allmennheten. I prinsippet betyr dette at en som skaper et åndsverk har enhver rett til å utnytte sitt verk. Dette inkluderer retten til å tilgjengeliggjøre verket på internett og selge det.

Det finnes likevel noen viktige unntak i åndsverkloven. Et av disse er unntaket i forhold til regelen om eksemplarfremstilling til privat bruk. Etter denne regelen er det lovlig å fremstille kopier av verk som er offentliggjort av rettighetshaveren (eksempelvis ved utgivelse av en cd, eller tilgjengeliggjøring på internett av musikk, film o.l.), til privat bruk. Dette følger av åndsverkloven § 12.

Uttrykket «privat bruk» er et skjønnsmessig og dynamisk uttrykk. Det vil i tillegg til den som selv har den rettmessige tilgangen til verket, omfatte familie og nære venner. Hva som ligger i dette, må fastlegges konkret i den enkelte sak. Helt klart er det at tilgjengeliggjøring til allmennheten ved bruk av internett er ulovlig dersom det ikke foreligger tillatelse fra rettighetshaveren til dette. Dette betyr i praksis at spredning av opphavsbeskyttede verk ved hjelp av fildelingstjenester (som «peer-to-peer») er ulovlig. Dersom man laster ned musikk eller annet opphavsbeskyttet materiale fra nettet som man vet er ulovlig delt, vil også dette være ulovlig etter åndsverkloven.

Det eksisterer utstrakte muligheter for å kopiere åndsverk som er lagret ved hjelp av datateknologi. Dette kan skje ved kopiering av dvd-er eller cd-er, opptak av radio- og fjernsynssendinger osv. En form for kopiering er at eksemplar av åndsverket konverteres til nytt format, for eksempel når

musikk kopieres fra cd til mp3-format. Når kopiering skjer minskes rettighetshaverens mulighet til å selge eksemplarer av åndsverket til mottakeren av kopien vesentlig. Det samme gjelder salg av eksemplarer på nye media, for eksempel salg av mp3-utgave av en musikkfil til dem som tidligere har kjøpt musikken på cd.

En undersøkelse foretatt av MMI for Norwaco i 2005, viser at 922.000 nordmenn i løpet av de siste syv dager før undersøkelsen ble foretatt hadde kopiert musikk. Totalt på denne uken ble det kopiert 35,4 millioner låter/musikkstykker, hvorav 21,6 millioner var ulovlig kopiert eller lastet ned.

For å forhindre kopiering eller konvertering fra blant annet dvd-er og cd-er der innehaver av opphavsretten ikke ønsker det, har medieprodusentene utstyrt sine produkter med såkalt DRM – Digital Rights Management. Dette er et teknisk system som er ment å begrense brukerens utnyttelse av innholdet, blant annet ved å hindre kopiering og konvertering.

Det har blitt opprettet nettbutikker som selger musikk for nedlasting i digitalt format. Dette er nettbutikker som opererer etter avtale med rettighetsinnehaverne, og som derved er lovlige. Enkelte av disse anvender DRM for å begrense mulighetene brukerne har til å anvende avspillingsutstyr som ikke er knyttet opp mot musikkleverandørens systemer.

Det er også et antall nettsteder som tilbyr musikk uten å ha avtale med rettighetshaveren og uten at rettighetshaveren får betaling. Lovstridig distribusjon av åndsverk i digital form og bruk av digitale åndsverk ved brudd på DRM, er sentrale områder innenfor datakriminalitet i dag. Det ligger imidlertid utenfor Datakrimutvalgets mandat å gå inn på de materielle reglene i åndsverksloven. Siden loven nylig er revidert og er basert på internasjonale regler antas det i hovedsak heller ikke å være noe stort behov for dette, selv om det hersker uenighet om rekkevidden av enkelte av bestemmelsene. Det vises til avgrensningene i kapittel 4.3 nedenfor. Datakrimutvalget har imidlertid vurdert om det bør foretas en samordning av enkelte bestemmelser i åndsverkloven med bestemmelser i straffeloven for så vidt gjelder vern av databasert informasjon, data og datasystemer. Dette harmoniseringsspørsmålet er belyst i kapittel 5.1.2 med videre henvisninger.

## 3.6 Spam

For at elektronisk kommunikasjon skal virke etter hensikten, er det viktig at kommunikasjonen er sikker, effektiv og til å stole på. I dag trues e-post og andre elektroniske kommunikasjonstjenester gjennom masseutsendelse av elektroniske meldinger som er uønskede for mottakeren. Den internasjonale betegnelsen på slik masseutsendelse er «spam». På norsk kalles det iblant «søppelpost».

Spam er meldinger som overføres via elektronisk kommunikasjon og til nå har e-posttjenesten vært den største kanalen for spam. Spamforsendelser utgjør stort volum idet hver melding blir sendt til mange mottakere på en gang. Meldingene kan sies å være uønsket siden mottakeren verken har bedt om eller gitt forhåndssamtykke til å motta dem. Utsending av meldinger er gjerne basert på adresselister hvor opplysningene er innsamlet i strid med personvernlovgivningen, og iblant også på annet ulovlig eller straffbart vis. Dessuten skjer utsendingen ofte ved at spamavsenderen misbruker en tredjeparts e-postserver (teknisk avsender). Dermed unngår spamavsender å belaste sitt eget datasystem med de automatiske bekreftelsene som sendes fra mottakernes datasystemer. Det store antallet bekreftelser kan i seg selv utgjøre så stor belastning at det kan gå ut over tilgjengeligheten på den tekniske avsenders datasystem. Ofte benyttes falsk avsenderadresse og tittellinje. Formålet er å omgå spamfiltre. En stor andel spam sendes som ledd i kommersiell markedsføring, men mye spam kan også knyttes til ulovlig virksomhet som bedragerier og piratomsetning av programvare, film og musikk. Spam kan også være bærer av skadelig dataprogram av forskjellig slag. Spam kan således være bærer av dataprogrammer med egenskaper som orm eller virus (se kapittel 3.4.8 om disse begrepene) som trenger inn på adressatenes datasystemer og skaper uautoriserte nett (botnet) eller annen skade, eller av program som skaper mer spam og genererer ytterligere stor belastning i nettet.

Spam utgjør et stort problem både med tanke på belastningen i kommunikasjonsnettene og for påliteligheten og tilliten til elektroniske kommunikasjonstjenester. Spam representerer også en stor økonomisk kostnad. Mange undersøkelser viser dette selv om det vanskelig kan foretas eksakte beregninger av omfanget. Det kan blant annet vises til at sikkerhetsfirmaene Symantec og MessageLabs har anslått at spam utgjør mellom 54 og 85 prosent av all e-post som sendes. OECD har i en rapport kalt «Anti-Spam Toolkit of Recommended Policies and Measures» av 13. april 2006, anslått at ca. 80 prosent av all e-post kan klassifiseres som spam. I 2005 vurderte Ferris Research kostnadene ved spam til 39 milliarder euro på verdensbasis, mens Computer Economic sitt anslag var at kost-

nadene ved spam og skadelig kode utgjorde ca. 11 milliarder euro på verdensbasis. Innenfor det Europeiske fellesskapet er bekjempelse av spam en prioritert sak.

I 2000 ble volumet av spam beregnet til 10 prosent av den totale e-post trafikken. De ovennevnte opplysninger viser således at det har skjedd en stor økning i problemets omfang de senere år. Årsaken er i stor grad at e-posttjenesten er et av de mest kostnadseffektive verktøy innenfor direkte markedsføring. Kostnadene er lave selv for et stort volum av utsendelser, og øker minimalt ved gjentatte henvendelser til samme mottaker. Bruk av spam er derfor lønnsomt selv om bare en liten andel av mottakerne faktisk blir reelle kunder. Kostnadene påvirkes heller ikke av avstander. Det kommer ut på ett om man sender e-post innenlands eller til en annen kant av verden. I tillegg er spam en effektiv metode for å spre skadelig dataprogram som nevnt ovenfor.

Det antas at spamproblemet vil bre seg til flere kommunikasjonstjenester dersom prisene på bruken faller slik at det blir økonomisk lønnsomt. For eksempel kan man tenke seg spam i tekstmeldinger over mobilnettet. Uansett er spam et problem ikke bare for e-post i dag, men også for news-grupper og telefaks, og det er et økende problem overfor nettsteder med interaktive funksjoner som blir benyttet som plattform for reklame (spam), som ikke er relatert til nettstedet selv (det er for eksempel en blogg).

Ulempene ved spam kan oppsummeres som følger:

- Spam kan utgjøre en så stor belastning i de elektroniske kommunikasjonsnettene at nettenes integritet blir truet, at overføringene går tregere og tilgjengeligheten til nett og tjenester blir redusert.
- Tilliten til e-post som tjeneste svekkes. For å bekjempe spam er det nødvendig å ta i bruk filtre (spamfilter), men slike filtre fungerer ikke med tilstrekkelig presisjon og stanser derfor også i en viss utstrekning legitime meldinger som skulle vært sluppet gjennom. Avsender kan derfor ikke nødvendigvis regne med at en e-post er kommet frem. Dette problemet anses å være i ferd med å ødelegge e-post som kommunikasjonstjeneste.
- Tiltak mot spam medfører kostnader for mottakerne, både for bedrifter og private.
- Spam hemmer effektiviteten i næringslivet og blir en tidstyv i privatlivet.
- Spam kan også anses som en krenkelse av privatlivets fred.

Det er bred internasjonal enighet om at spam må bekjempes ved en kombinasjon av tiltak, det vil si ved bruk av lovregulering, bevisstgjøring av brukerne, tekniske løsninger, selvregulering og internasjonalt samarbeid. I den nevnte OECD-rapporten om tiltak mot spam, er effektive sanksjoner fremhevet som et nødvendig virkemiddel. Lovgivningen må altså utvikles med sikte på å oppnå dette. Den strafferettslige tilnærming til problemet er drøftet i kapittel 5.6.6.

## 3.7 Uønsket innhold på internett

### 3.7.1 Innledning

Internetts funksjonalitet innebærer en tilvekst i måten man kan formidle ytringer og tjenester av alle slag til alle verdenshjørner på. Enhver kan publisere ytringer uten tilgang på kapital, trykkefasiliteter og øvrig distribusjonsnett. Den senkede publiseringsterskelen, som er en konsekvens av dette, innebærer imidlertid også at useriøse aktører har vid tilgang til publisering.

Bruk av internett innebærer ofte grenseoverskridende handlinger. Ulik lovgivning i ulike geografiske områder er med andre ord ofte knyttet til samme publiseringshandling. Gjerningspersonene setter gjerne opp sine tjenester eller publiserer sine meninger via tjenesteytere i land hvor det er mindre sannsynlig at man blir straffeforfulgt eller hvor den aktuelle handlingen ikke anses som ulovlig. Det vises til redegjørelsen i kapittel 8.

I det følgende omtales noen av de viktigste og mest velkjente typer av uønsket innhold på internett.

### 3.7.2 Seksualiserte skildringer av barn

Ved lovendring av 20. juni 2005 nr. 29 ble seksualiserte skildringer av barn skilt ut i en egen bestemmelse i straffeloven § 204a. Stortinget fremhevet også i den forbindelse at seksualiserte skildringer av barn ikke er alminnelig pornografi, men en skildring av overgrep mot barn. Den nye bestemmelsen rammer videre enn § 204, som er rettet mot den «alminnelige pornografi».

I enkelte miljøer av overgripere fungerer slikt materiale som valuta som gir adgang til tjenester, eller som kan benyttes som byttemiddel for å erverve ytterligere materiale.

En vanlig fremgangsmåte for profittmotiverte tilbydere av seksualiserte skildringer av barn, er å tilgjengeliggjøre materialet på webservere hvor

brukere kan logge seg på mot betaling for å få tilgang.

En effektiv måte å spre og skaffe seg ulovlig materiale på, er gjennom ulike fildelingstjenester. Såkalte nyhetstjenester er eksempler på dette. Dette tilbys av tjenesteytere. Brukere kan poste «nyheter» i ulike nyhetsfora. Disse nyhetene kan inneholde bilder, eller lenker til ressurser på nettet osv. En annen type fildeling som skiller seg fra nyhetstjenestene, er peer-to-peer-tjenester. Slike tjenester er programmer som gjør det mulig å søke gjennom innhold på andre brukeres datamaskiner, og å laste ned materiale som deles av andre brukere direkte fra deres maskiner. Tjenestene er ikke lagt opp til å identifisere brukerne. Tvert i mot er programmene under tiden lagt opp med funksjoner som er ment å skjule brukernes identitet.

I tillegg finnes det også en rekke forskjellige chattetjenester med egne kanaler dedikert til pornografi og/eller seksualiserte skildringer av barn. Her kan man bytte bilder, filmer, informere andre om lenker til steder med det aktuelle materialet osv. For å få tilgang til enkelte av disse kanalene må man ha et passord eller bli invitert av andre brukere. Som nevnt ovenfor kan da egen samling av pornografisk materiale fungere som betalingsmiddel for å få tilgang til slike kanaler.

I 2004 opprettet Kripos i samarbeid med Telenor et filter for å fange opp seksualiserte skildringer av barn på nettet. Dette er en frivillig ordning som de ulike internettleverandørene kan være med på. Kripos oppdaterer fortløpende en liste over ulike nettsteder som inneholder seksualiserte skildringer av barn. Listen distribueres til internettleverandørene, som på grunnlag av denne hindrer tilgang for sine brukere til de aktuelle sidene. Filteret er lagt opp slik at det bare er effektivt mot websider. Det hindrer ikke spredning av denne typen skildringer gjennom for eksempel chattekanaler (IRC), fildeling (peer-to-peer) eller nyhetstjenester. Selv om filteret er frivillig, har norske internettilbydere blitt med på ordningen, som av den grunn er forholdsvis effektiv. Likevel er det fortsatt muligheter for å få tilgang fra Norge til mange sider med seksualiserte skildringer av barn. Det kommer stadig til nye sider, og det tar noe tid før disse blir fanget opp og kommer inn på listene til Kripos. Det er nok også slik at ikke alle sidene blir oppdaget, og dermed heller ikke kommer med på listen. Dessuten fanger ikke filteret opp distribusjon via e-post og liknende.

Seksualiserte skildringer av barn er forøvrig regulert i datakrimkonvensjonens artikkel 9. I Datakrimutvalgets delutredning I (NOU 2003: 27) er forholdet til denne bestemmelsen behandlet på sidene 24-25.

Utvalget har valgt å avgrense mot videre behandling av dette problemområdet i den videre fremstillingen, og viser til kapittel 4.3.2. I kapittel 5.13 drøftes hvorvidt det foreligger et behov for generelle regler om filtrering.

### 3.7.3 Ærekrenkelser på nett

De norske straffebestemmelsene om ærekrenkelse finnes i nåværende straffelov §§ 246 flg. Anvendelsesområdet for disse reglene må ses i sammenheng med det grunnleggende prinsipp om ytringsfrihet i norsk rett. Disse prinsippene kommer til uttrykk i Grunnloven § 100 og EMK artikkel 10. Bestemmelsene om ærekrenkelse er medienøytrale, og ærekrenkelser bedømmes ikke annerledes om de fremsettes på internett eller i andre fora. Utvalget går derfor ikke nærmere inn på dette i utredningen.

### 3.7.4 Personbilder på nett

Grunnet stadig bedre og billigere teknologi er det nå svært mange som har det nødvendige utstyr for enkelt å publisere bilder på internett. En stor del av befolkningen har mobiltelefoner med kamera tilgjengelig. Dermed er det stadig lettere å fotografere situasjoner, mennesker og annet som man kommer over tilfeldig.

Publisering av personbilder, også på internett, er beskyttet av den alminnelige ytringsfriheten, jf. Grunnloven § 100 og EMK artikkel 10. Norsk rett oppstiller dog begrensninger i retten både til å ta, og særlig til å publisere bilder av personer. Bestemmelser som kan tenkes anvendt i denne sammenheng er blant annet straffeloven §§ 204, 204a, 390 a og bestemmelsene om ærekrenkelse i straffeloven §§ 246 flg. Andre lover er personopplysningslovens bestemmelser og bestemmelsen i domstolloven § 131a.

En sentral bestemmelse, som vil ha særlig aktualitet når det gjelder publisering på internett, er åndsverkloven § 45c. Det er særlig reglene i første ledd bokstav a-c som er av interesse. Disse lyder slik:

> Fotografi som avbilder en person kan ikke gjengis eller vises offentlig uten samtykke av den avbildede, unntatt når
> a) avbildningen har aktuell og allmenn interesse,
> b) avbildningen av personen er mindre viktig enn hovedinnholdet i bildet,

c) bildet gjengir forsamlinger, folketog i friluft eller forhold eller hendelser som har allmenn interesse.»

Omfanget av bilder som kan være ulovlig publisert på internett er stort. Ved bruk av søkeord som «fest», «bilder», «party» og lignende, får man i de fleste søkemotorer enkelt adgang til tusentalls sider der det finnes bilder av personer som fremstår som overstadig berusede, befinner seg i mer eller mindre private situasjoner, sovende osv. Ofte er personene på bildet navngitt. Det er nok ikke tvilsomt at for en rekke av disse bildene, er det ikke gitt samtykke av den som er avbildet. Dette er heller ikke bilder av allmenn interesse, eller bilder som på annen måte faller inn under unntakene i åndsverkloven § 45c.

Et annet problem er at mindreårige ofte laster opp bilder av seg selv, mange ganger i dristige settinger, uten samtykke fra sine foresatte. Det må antas at personer under 15 år i hvert fall må ha samtykke fra foresatte, jf. barneloven kapittel 5 og retningslinjer på Datatilsynets nettsider.

Dersom den som er avbildet ønsker å få bildet sitt fjernet fra nettet, vil man kunne pålegge den som først publiserte dette å fjerne det fra sin webside. Det samme kan man med andre nettsteder hvor det er kjent at bildet er. Innen dette blir gjort, er det dog en stor sjanse for at bildet er sett av tusenvis av nettbrukere, kanskje lastet ned og lagret steder det er nærmest umulig å finne frem til, og skaden har da allerede skjedd. Slike bilder kan dukke opp igjen lang tid etter de ble tatt, og være svært plagsomt for den eller de som er avbildet.

Utvalget følger ikke opp disse problemstillingene i denne delutredningen. Utvalget har vurdert egne paragrafer i straffeloven som gjelder publisering på internett, men tiden har ikke tillatt å fullføre utredningen av dette. Det foreligger dessuten mange regler om dette i spesiallovgivningen. Det vises for øvrig til avgrensningene som er gjort i kapittel 4.3.3.

### 3.7.5 Personopplysninger på nett

Så vel næringsdrivende som offentlige myndigheter benytter i økende grad internett til å innhente og ta i bruk personopplysninger fra publikum/forbrukere. Slik behandling av personopplysninger er en naturlig og selvfølgelig del av den virksomhet disse driver. Dette innebærer en risiko både for misbruk fra dem som mottar opplysningene, og for at noen uten legitim interesse får tak i slike opplysninger som er lagret eller overføres elektronisk. Personopplysninger på avveie kan lett benyttes som middel i identitetstyverier, som igjen kan åpne for en rekke andre kriminelle handlinger som blant annet bedrageri. I Norge er tilegnelsen og bruken av personopplysninger regulert i flere forskjellige lovbestemmelser, særlig i personopplysningsloven.

Personopplysningsloven har i mange sammenhenger stor betydning for reguleringen av hva det er adgang til å publisere på internett. Blant annet må det, etter at EU-domstolen behandlet den såkalte Lindquist-saken fra Sverige, antas at publisering av personopplysninger på internett, også på private hjemmesider, ikke kan gjøres uten samtykke fra de involverte. I den nevnte saken hadde en person på en nettside tilhørende en menighet lagt ut opplysninger om navn, arbeidsoppgaver, fritidsinteresser, helsetilstand m.v. hos medarbeidere i menigheten. Dette ble ansett for å være i strid med den svenske personopplysningsloven, som tilsvarer den norske.

Som nevnt under 3.7.3, har Datakrimutvalget vurdert å foreslå egne bestemmelser i straffeloven som gir en samlet regulering av publisering på internett, men ikke funnet tid til å utarbeide et slikt forslag. Det avgrenses derfor også på dette punktet mot videre behandling av spørsmålet.

### 3.7.6 Pengespill på internett

Norsk spillepolitikk er tuftet på en forsiktighetslinje hvor det er lagt stor vekt på en sosialpolitisk forsvarlig utforming av det samlede spilletilbudet.

Når det gjelder lykkespill på internett er det fra Kultur- og Kirkedepartementet i Ot.prp. nr. 44 (2002-2003) side 45 uttalt:

> «Etter norsk lovgivning er det forbudt å avholde lotterier og pengespill uten tillatelse eller særskilt hjemmel i lov. Rekkevidden av norsk lov er som hovedregel begrenset til norsk territorium. Utenlandske lotteri er dermed ulovlige etter norsk rett i den grad de avholdes på norsk territorium. Også lotteri som avholdes i Norge via Internett vil være avhengig av norsk tillatelse for å være lovlig i Norge. Det vil imidlertid ikke være ulovlig å delta i lotteriet fra terminal i Norge selv om lotteriet ikke har norsk tillatelse.
>
> Et sentralt spørsmål er imidlertid om selve framsendelsen av lotteri og pengespill fra server i utlandet kan sies å være ulovlig avholdelse av lotteri og pengespill i Norge. Etter departementets vurdering foreligger det ikke en entydig internasjonal oppfatning av de nasjonale rettsreglenes rekkevidde i forhold til pengespilltilbud som framsendes via Internett fra

utenlandske spilltilbydere. Den svensk utredningen Från tombola till Internett - översyn av lotterilagsstiftningen (SOU 2000:50) konkluderer med at svensk rett ikke forbyr framsendelse av lotteritilbud på Internett fra utlandet til Sverige. Gjeldende svenske regler tilsvarer de norske på dette området. På den annen side har det danske Skatteministeriets utredning Spil i fremtiden - overveielser om en samlet spillelovgivning fra april 2001 konkludert med at et utenlandske spilletilbud omfattes av det danske straffbelagte forbud mot spilletilbud uten tillatelse, dersom tilbudet kan sies å ha virkning i Danmark. Utgangspunktet for den danske konklusjonen er det såkalte virkningsprinsippet i dansk strafferett. Prinsippet innebærer at en straffbar handling, hvor straffbarheten avhenger eller påvirkes av en inntrådt eller tilsiktet følge, anses begått også der hvor handlingen er inntrådt eller tilsiktes å inntre. Et identisk prinsipp gjelder i norsk strafferett etter straffeloven § 12 annet ledd. Departementet er imidlertid ikke kjent med at nasjonale forbudsbestemmelser er håndhevet overfor utenlandske pengespill ut fra den betraktning at Internettilbudet i seg selv må anses å ha virkning i mottakerlandet.»

Det er særlig pokerspill på nettet som har hatt en kraftig oppblomstring de siste årene. Når det gjelder poker generelt, har Lotteri- og Stiftelsestilsynet uttalt at det oppfyller kriteriene for tilfeldighet, som er nødvendig for å anses som lotteri i lovens forstand. Dersom det koster noe å delta og man har en mulighet for gevinst, er pokeraktiviteten ulovlig selv om det er i privat regi.

Nordmenn over 18 år brukte ifølge tall fra Lotteri- og Stiftelsestilsynet 4,7 milliarder kroner til pengespill over internett i 2005. Vel 700 millioner av dette ble brukt på Rikstotos og Norsk Tippings online-spill, og dermed er estimatet på utenlandske, uregulerte og ikke-tillatte spill på ca. 4 milliarder kroner i 2005. Totaltallet for nordmenns bruk på regulerte pengespill på og utenfor internett var 41,7 milliarder kroner i 2005.

Straffeloven §§ 298 og 299 inneholder straffebestemmelser angående lykkespill (spill om penger og veddemål). I tillegg har vi straffeloven § 383. Disse bestemmelsene er ikke foreslått videreført i den nye straffeloven. Det vises til NOU 2002: 4 side 412 og side 423. Straffelovkommisjonen mener at disse spørsmålene bør reguleres av lotteriloven (lov av 24. februar 1995) og pengespilloven (lov av 28. august 1992 nr. 103). Datakrimutvalget er enig i dette, og har derfor avgrenset mot videre utredning av denne problematikken i denne delinnstillingen.

### 3.7.7 Seksualiserte, voldelige og øvrige uønskede dataspill

Dataspill spilles på håndholdte enheter som mobiltelefoner, på hjemmedatamaskiner, og på spesiallagede spillmaskiner. Alle disse systemene kan kobles sammen i nettverk, slik at man kan spille mot andre i lukkede nettverk eller over internett.

Omsetning av dataspill er i dag ikke spesifikt regulert av norsk lov når det gjelder forhåndssensur eller absolutte aldersgrenser. Innholdet i enkelte dataspill kan stride mot alminnelige samfunnsnormer. Som i bildemediene generelt gjelder dette spesielt fremstillinger av vold og sex, samt moralsk tvilsomme handlinger. Hensynet til beskyttelse av barn og unge tilsier at dette må tas på alvor.

Dataspill omfattes av straffeloven § 382 som retter seg mot den som «utgir eller frambyr til salg eller leie eller på annen måte søker å utbre» dataspill «hvor det i underholdningsøyemed er gjort utilbørlig bruk av grove voldsskildringer». Straffeloven § 382 er av straffelovkommisjonen foreslått videreført som § 21-8 i ny straffelov.

Datakrimutvalget har ikke fremmet noe lovforslag som retter seg spesifikt mot slike dataspill. Emnet ligger utenfor kjerneområdet av det utvalget har konsentrert seg om i denne delutredningen, og tiden har ikke tillatt å gå nærmere inn på denne problematikken.

### 3.7.8 Forbudte ytringer på internett

I Norge hører ytringsfriheten med blant de grunnleggende prinsipper i konstitusjonen. Ytringsfriheten står også sentralt i den europeiske menneskerettskonvensjonen. Det er likevel grenser for ytringsfriheten, som blant annet kommer til uttrykk i straffeloven § 135 a.

Utgangspunktet er at rammene for ytringsfrihet er den samme på internett som ellers. Dette kompliseres imidlertid av internetts internasjonale karakter.

Tilleggsprotokoll av 28. januar 2003 til datakrimkonvensjonen inneholder regler som medfører begrensninger i ytringsfriheten der ytringene foretas ved hjelp av datasystem. Protokollen gjelder rasistiske eller fremmedfiendtlige handlinger. Forholdet mellom denne protokollen og norsk rett drøftes nærmere i kapittel 7.

Et annet problemområde er når norsk lov får anvendelse og når saker kan fremmes for norske domstoler for så vidt gjelder ytringer fremsatt over internett. Problemstillingen knytter seg særlig til ytringer nordmenn har fremsatt ved bruk av ser-

vere som er plassert utenfor Norge og til ytringer som er fremsatt av utlendinger, men som er tilgjengelig i Norge. Utvalget behandler disse aspektene i kapittel 8.

Selv om gjerningspersonen befinner seg utenfor norsk jurisdiksjon, kan man tenke seg straffesanksjonert medvirkeransvar mot personer som befinner seg innenfor norsk jurisdiksjon. Dette behandles i kapittel 5.11. Tiltak som filtrering kan også brukes for å skjerme norsk sektor mot uønsket innhold; se kapittel 5.13.

# Kapittel 4
# Rettslige utgangspunkter

## 4.1 Et eget kapittel om datakriminalitet

### 4.1.1 Begrepet «datakriminalitet»

Etter en alminnelig forståelse omfatter uttrykket «datakriminalitet» både kriminalitet som er rettet mot data og datasystemer, og kriminalitet hvor datautstyr benyttes som verktøy for å begå handlingen. Utvalget har ikke sett behov for å gi uttrykket «datakriminalitet» en rettslig definisjon. Mandatet sett under ett oppfattes som et oppdrag om å gi regler om kriminalitet som har sammenheng med bruk og utnyttelse av datateknologi (IKT). Begrepet datakriminalitet er hensiktsmessig for å indikere hva lovforslaget gjelder.

### 4.1.2 Særregulering av datakriminalitet eller inkorporering i andre deler av straffeloven?

Et viktig systematisk spørsmål har vært å ta stilling til om det skal gis særlige straffebestemmelser om datakriminalitet eller om alternativer som rammer slike handlinger bør inkorporeres i de øvrige straffebestemmelsene. Ved Straffelovrådets revisjon av straffeloven med tanke på datakriminalitet i 1985-1987, ga mandatet en føring om at man så langt som mulig skulle basere seg på de alminnelige bestemmelsene. Denne systematikk ble da også valgt, se NOU 1985: 31 «Datakriminalitet» side 5 og 28, og Ot.prp. nr. 35 (1986-1987) side 13.

Mandatet av 6. september 2005 stiller Datakrimutvalget fritt med hensyn til systematisk plassering av straffebudene, og i dag er nok erfaringen at krenkelser mot data og datasystemer reiser så mange særlige spørsmål at man er best tjent med en særregulering.

Utvalget foreslår å samle reglene om datakriminalitet i et eget kapittel kalt «Vern av data, databasert informasjon og datasystemer» i ny straffelov. For det første anvendes visse sentrale begrep i flere av bestemmelsene, noe som har gitt behov for å innta legaldefinisjoner i lovutkastet § 1. Regler som anvender definisjonene bør stå samlet, tilsvarende systematikken i straffeloven kapittel 18 om dokumentfalsk, hvor straffebudene står plassert i umiddelbar tilknytning til legaldefinisjonen i straffeloven § 179 i begynnelsen av kapitlet. Straffelovkommisjonen foreslo å videreføre denne systematikken for dokumentfalsk, se utkast til kapittel 31 om vern av tilliten til dokumenter og penger i NOU 2002: 4 Ny straffelov (delutredning VII), side 374 flg. Utvalgets forslag til kapittel om vern av data, databasert informasjon og datasystemer føyer seg inn i en tilsvarende systematikk.

Datakrimreglene har et innbyrdes slektskap. Pedagogiske hensyn og hensyn til oversiktlighet tilsier at de plasseres samlet. Det gjør det enklere å sette seg inn i strafferegulering på et område som kan oppfattes som vanskelig tilgjengelig. Lovforslaget dekker ulike stadier og sider ved den straffverdige atferd som det ofte vil være hensiktsmessig å se under ett. For eksempel er det naturlig at regler om ulovlig tilgang til datasystem (utkastet § 4) og data- og informasjonstyveri (utkastet §§ 5 og 6) står i nærheten av hverandre siden slike handlinger ofte vil følges ad. Straffebudene har imidlertid slektskap med andre bestemmelser også, for eksempel innbrudds- og tyveribestemmelsene i straffeloven §§ 147 og § 257. Inkorporering er imidlertid ikke nødvendigvis den mest hensiktsmessige lovteknikken fordi datakriminalitet reiser egne spørsmål som uansett må løses. Datatyveri kan illustrere dette. Datatyveri skjer ved uberettiget kopiering eller overføring av data til datasystemer som gjerningspersonen kontrollerer. Ved eventuell inkorporering av utkastet § 6 (datatyveri) i straffeloven § 257, oppstår problemer i forhold til vilkårene «gjenstand» og «borttar». Det vises også til fremstillingen i Sunde 2006 «Lov og rett i cyberspace» kapittel 4 om dette.

Det antas at utbygging av andre straffebud med alternativer som dekker datakriminalitet, vil kunne gjøre dem svært kompliserte. Det er heller ikke gitt at legaldefinisjonene i utkastet § 1 er hensiktsmessige for andre straffebud i den spesielle del, som måtte inneholde tilsvarende uttrykk. Definisjonene er utarbeidet med tanke på bestemmelsene i datakrimkapitlet, ikke på de øvrige straffebudene i den spesielle delen. Til slutt pekes det på at med en selvstendig regulering får man bedre frem de spesielle legislative hensyn som gjør seg

gjeldende ved beskyttelse av data utover de som gjelder formuesgoder mer generelt, se kapittel 4.6.2 om datasikkerhetshensynene.

I Straffelovkommisjonens delutredning VII ble datakrimbestemmelsene foreslått samlet i ett kapittel om vern av informasjon og informasjonsutveksling i utkastet kapittel 23, side 318 flg. Etter kommisjonens forslag inneholdt kapitlet også andre bestemmelser (enn datakrimbestemmelser) til vern om det samme, blant annet straffebud om brudd på taushetsplikt (VII utkast til § 23-1), brudd på bedriftshemmelighet (VII utkast til § 23-6) og åpning eller hindring av brev m.v. (VII utkast til § 23-10). Også utkastet til straffebud om offentliggjøring av private forhold (VII utkast til § 23-2), som er en videreføring av straffeloven §§ 248 nr. 2 og 390, kan nevnes. For de øvrige dataspesifikke bestemmelsene fulgte det av kommisjonens forslag at disse bare kunne overtres ved tekniske metoder, for eksempel ved misbruk av datasystem og avlyttingsutstyr m.v. Datakrimutvalgets forslag til særregulering skiller seg fra kommisjonens ved at straffebud som ikke er satt til vern om data, databasert informasjon eller datasystemer, eller som etter gjerningsbeskrivelsen tydelig rammer handlinger som begås ved hjelp av datateknologi, foreslås skilt ut til andre kapitler i ny straffelov. Utvalget er imidlertid enig med kommisjonen i at dataspesifikke straffebud forutsettes overtrådt ved dataspesifikke fremgangsmåter, og følgelig skal kunne anvendes i konkurrens med andre straffebud, der det er naturlig. Se som eksempel delutredning VII side 325, utkastet § 23-11 om skadeverk på elektronisk lagret informasjon, hvor det opplyses at

> «informasjon kan også gå tapt ved fysisk ødelegging av lagringsmediet, for eksempel hvis en datamaskin blir knust med en slegge. I så fall vil bestemmelsene om skadeverk på informasjon kunne anvendes i konkurrens med bestemmelsene om skadeverk på fysiske ting [...]»

Utvalget slutter seg til dette.

Ytterligere har utvalget sett hen til det praktiske behovet for oppdatering av straffebudene. Teknologi- og samfunnsutvikling går raskt og det antas at teknisk betonte straffebud jevnlig må gjennomgås for å påse at de er relevante og anvendelige. Det er påregnelig at nye straffverdige utnyttelsesformer vil oppstå i fremtiden. Kontrollen gjøres enklere dersom reglene er plassert i sammenheng. Styrken av dette hensynet avhenger imidlertid av gjerningsbeskrivelsene. Dersom de er tilstrekkelig generelt og fleksibelt utformet og beskriver modus snarere enn misbruk av spesifikke tjenester, antas de også å kunne ha en viss tidsbestandighet. På den annen side setter legalitetsprinsippet grenser for hvor generelt straffebud kan utformes. Dersom generaliserings- eller abstraksjonsnivået blir for høyt, fratas straffebudene også noe av de pedagogiske og opplysende funksjoner. Det synes naturlig i hvert fall å planlegge for et revisjonsbehov på dette feltet med jevne mellomrom. Også av denne grunn antas det at det er hensiktsmessig at bestemmelsene står samlet.

Spørsmålet om plasseringen av straffebudene om datakriminalitet beror først og fremst på hva som anses hensiktsmessig. Som det fremgår har utvalget lagt avgjørende vekt på hensynene til reglenes innbyrdes sammenheng, felles begrepsbruk, pedagogiske formål, behovet for oversiktlighet og det antatte oppdateringsbehovet. Disse hensynene tilsier særregulering i et eget kapittel. Straffebudene i dette kapitlet gjelder bare handlinger i kjerneområdet for datakriminalitet. Kapitlet omfatter ikke straffebud hvor bruk av data bare er en av flere mulige måter å begå overtredelsen på. Slike handlinger fanges opp av andre straffebud hvor gjerningsbeskrivelsen er utformet mer generelt, og som snarere lar den vernede interesse være avgjørende for straffbarheten fremfor den konkrete fremgangsmåte som ble benyttet. Det vises for eksempel til straffeloven § 135 a om spredning av straffbare ytringer, straffeloven § 204a om befatning med seksualiserte skildringer av barn, og straffeloven § 390 a om krenkelse av privatlivets fred.

Utenfor kapitlet om vern av data, databasert informasjon og datasystemer legger utvalget frem forslag til supplering av reglene i ny straffelov kapittel 13 om inndragning (utkastet §§ 76a og 76b). Det fremlegges også en skisse til regler om dokumentfalsk i relasjon til data, som foreslås tatt inn i kapitlet om vern av tilliten til dokumenter og penger i ny straffelov. For en fullstendig oversikt over lovforslaget vises det til kapittel 5.1.

## 4.2 Historikk om bestemmelsene om datakriminalitet – tidligere utredningsarbeid

### 4.2.1 Dataspesifikke endringer

I 1985 ble straffeloven gjennomgått med tanke på om den ga tilfredsstillende dekning mot datakriminalitet. Straffelovrådet avga utredningen NOU 1985: 31 «Datakriminalitet». Arbeidet ledet til visse endringer i straffeloven ved endringslov av 12. juni

1987 nr. 4. Endringene var som følger: Straffeloven § 151 b (sabotasje) ble tilføyd. Regelen om datainnbrudd ble gitt en modernisert ordlyd og skilt ut som eget ledd i straffeloven § 145 annet ledd. Det ble tatt inn en bestemmelse om uberettiget bruk av løsøregjenstand i straffeloven § 261, og tilføyd en bestemmelse om databedrageri i straffeloven § 270 første ledd nr. 2.

I 1995 ble det på ledig plass i straffeloven tilføyd et straffebud i § 262 til vern om betalingsbelagte kodete kringkastingssignaler, jf. lov av 7. april 1995 nr. 15. Bestemmelsen ble tatt inn fordi det gjennom to høyesterettsdommer var fastslått at det ikke forelå et tilfredsstillende strafferettslig vern mot såkalt piratdekoding av fjernsynssendinger, verken etter straffeloven § 145 annet ledd, eller etter åndsverklovens regler, se Rt. 1994 side 1610 (Betal-tv-dommen) og Rt. 1995 side 35 (Smartkort-dommen). Ved lovendring av 15. juni 2001 nr. 57, ble straffeloven § 262 bygd ut til sin nåværende form. Straffebudet gjelder piratvirksomhet overfor såkalte vernede tjenester. Vernet tjeneste er legaldefinert i straffeloven § 262 fjerde ledd, og omfatter betalingsbelagte tilgangskontrollerte kringkastingssignaler og informasjonssamfunnstjenester. Bestemmelsen rammer forskjellige spesifiserte medvirkningsformer til piratdekoding (første ledd), og piratdekoding som sådan (annet ledd). Endringene ble foretatt for å gjennomføre kravene i tilgangskontrolldirektivet av 20. november 1998 (98/94 EF) og tilgangskontrollkonvensjonen av 24. januar 2001 (ETS 178).

Den 23. november 2001 undertegnet Norge Europarådskonvensjonen Convention on Cybercrime (ETS 185) («datakrimkonvensjonen»). Som følge av tiltredelsen nedsatte regjeringen Datakrimutvalget. Datakrimutvalget leverte utredningen NOU 2003: 27 «Lovtiltak mot datakriminalitet». Utredningen gir anvisning på de lovendringer som er nødvendige for å oppfylle datakrimkonvensjonens minimumskrav, og gir ikke anbefalinger utover dette. På bakgrunn av datakrimkonvensjonen artikkel 9, ble også bestemmelsen om seksualiserte skildringer av barn i daværende bestemmelse i straffeloven § 204 gjennomgått, uten forslag om å endre denne.

Gjennomføring av datakrimkonvensjonens krav skjedde ved endringslov 8. april 2005 nr. 16. Følgende endringer i straffeloven ble gjort:

– Straffeloven § 12 første ledd nr. 3 bokstav a: Straffeloven §§ 145 annet ledd og 145b ble tilføyd i opplistingen av bestemmelser. Slike overtredelser er derfor straffbare også når de er begått i utlandet av norsk statsborger eller en i Norge hjemmehørende person.
– Straffeloven § 145 annet ledd: Beskyttelsesvilkåret ble fjernet. Bestemmelsen ble dermed endret fra en beskyttelsesbruddsbestemmelse til en datavernbestemmelse. I tillegg ble strafferammen forhøyet fra «bøter eller med fengsel inntil 6 måneder», med tilføyelsen av alternativet «eller begge deler». Formålet var å hindre rask foreldelse og gi mulighet for økt bruk av tvangsmidler.
– Straffeloven § 145b: Det ble tilføyd en ny bestemmelse om spredning av tilgangsdata.

Videre må endringene i åndsverkloven ved endringslov 17. juni 2005 nr. 97 nevnes. Endringene ble foretatt for å gjennomføre to WIPO konvensjoner av 20. desember 1996, henholdsvis the Copyright Treaty og the Performances and Phonograms Treaty, samt krav i opphavsrettsdirektivet (direktiv 2001/29/EF av 22. mai 2001) i norsk rett. Lovendringsarbeidet gjaldt først og fremst problemstillinger knyttet til vern og distribusjon av digitaliserte åndsverk, herunder rettslig vern for systemer for elektronisk rettighetsadministrasjon («digital rights management» – DRM).

Av spesiell betydning i forhold til datakriminalitet er tilføyelsen av åndsverkloven § 53a, lest i sammenheng med presiseringen av eneretten i § 2 annet til fjerde ledd. Bestemmelsen er straffesanksjonert, jf. åndsverkloven § 54 første ledd bokstav b. Bestemmelsen gjelder forbud mot omgåelse av tekniske beskyttelsessystemer til vern om digitaliserte åndsverk, og slår til dels inn på området for straffeloven § 145 annet ledd (vern om data), straffeloven § 145b (spredning av tilgangskoder) og straffeloven § 262 (vernede verk). Også den eldre bestemmelsen i åndsverkloven § 54a, som ble renummerert til åndsverkloven § 53c, har slektskap med de nevnte reglene.

### 4.2.2 Seksualiserte skildringer av barn

Parallelt med Datakrimutvalgets arbeid pågikk en lovendringsprosess for å styrke barns rettigheter. Bakgrunnen var det generelle behovet for økte tiltak på området, påvist blant annet i Seksuallovbruddutvalgets utredning NOU 1997: 23 «Seksuallovbrudd». Dette sammenfalt med en vesentlig rettslig utvikling på det internasjonale plan, især ved vedtagelsen av FNs tilleggsprotokoll til barnekonvensjonen av 25. mai 2000 om salg av barn, barneprostitusjon og barnepornografi, samt EUs rammebeslutning om bekjempelse av seksuell utnytting av barn og barnepornografi av 22. desember 2003 (2004/68/JHA). Denne prosessen resulterte blant annet i flere suksessive endringslover som justerte rekkevidden av forbudet mot seksualiserte skildringer av barn.

Etter det nevnte utredningsarbeidet fremmet regjeringen to lovproposisjoner om datakriminalitet og styrking av barns rettigheter. Ot.prp. nr. 40 (2004-2005) fulgte opp Datakrimutvalgets arbeid, mens Ot.prp. nr. 37 (2004-2005) (eige straffebod om kjønnslege skildringar som gjer bruk av barn) gjaldt styrking av barns rettigheter. Lovforslaget i den sistnevnte proposisjonen dekket også kravene etter datakrimkonvensjonen artikkel 9.

– Som følge av utredningsarbeidet i Ot.prp. nr. 37 (2004-2005) ble forbudet mot seksualiserte skildringer av barn skilt ut som egen bestemmelse og vesentlig omarbeidet, jf. straffeloven § 204a. Endringen skjedde ved lov av 20. mai 2005 nr. 29. Straffebudet tilfredsstiller kravene i datakrimkonvensjonen artikkel 9, uten bruk av reservasjonsadgangen i artikkel 9 nr. 4.

#### 4.2.3 Arbeidet med ny straffelov

Ny straffelov alminnelig del ble vedtatt ved lov 20. mai 2005 nr. 28. Til grunn for dette arbeidet ligger særlig Ot.prp. nr. 90 (2003-2004) og Innst.O. nr. 72 (2004-2005). I henhold til mandatet skal Datakrimutvalget gjennomgå enkelte av de bestemmelser som ble vedtatt i alminnelig del, særlig bestemmelsene om straffelovens stedlige virkeområde, jf. ny straffelov §§ 4-7. Utvalget har også sett på reglene om rettighetstap og inndragning.

Straffelovkommisjonens skisse til straffebud i kapitlet om Vern av informasjon og informasjonsutveksling etablerer et generelt informasjonsvern som gjelder informasjon representert både i elektroniske data og på annen måte, for eksempel på papir. Se delutredning VII side 318 flg. om utkast til kapittel 23. Datakrimutvalget går inn for at bare dataspesifikke bestemmelser inntas i samme kapittel. Det antas at de øvrige bestemmelsene i delutredning VII utkastet kapittel 23 kan følges opp andre steder i ny straffelov.

Utvalget har ellers forholdt seg til forarbeidene til ny straffelov og til de alminnelige bestemmelsene i ny straffelov. Utvalget har bare behandlet spørsmål som ligger innenfor den avgrensningen som fremgår nedenfor.

### 4.3 Avgrensning av mandatet

#### 4.3.1 Straffebud til vern av data, databasert informasjon og datasystemer

Mandatet gir utvalget stor frihet i utformingen av lovforslaget. Utvalget mener det er sentralt å lage bestemmelser til vern av data, databasert informasjon og datasystemer, jf. annet punkt i mandatet. Dette omfatter etter en naturlig forståelse regler som beskytter påliteligheten og tilliten til datasystemer og den informasjon som der behandles. Det er således tale om straffebud mot uberettiget tilgang til datasystemer, uberettiget tilegnelse av data og databasert informasjon, uberettiget bruk av datasystemer, skadevoldende handlinger rettet mot data og datasystemer osv.

#### 4.3.2 Om gjeldende straffelov i tilstrekkelig omfang og tilstrekkelig strengt straffer handlinger som begås ved misbruk av data og datasystemer

Videre har utvalget vurdert om den gjeldende straffelov i tilstrekkelig omfang og tilstrekkelig strengt straffer handlinger som begås ved misbruk av data og datasystemer, jf. tredje punkt i mandatet. Databedrageri er et eksempel på en straffbar handling som naturlig omfattes av denne del av mandatet. Men her gis det også foranledning til å vurdere en lang rekke andre straffbare handlinger siden svært mange handlinger kan begås elektronisk så vel som fysisk. Noen eksempler er spredning av seksualiserte skildringer av barn, jf. straffeloven § 204a, trusler, jf. straffeloven § 227, krenkelser av privatlivets fred, jf. straffeloven § 390 a, uberettiget tilegnelse og bruk av bedriftshemmeligheter, jf. straffeloven § 294 nr. 2 og 3, dokumentfalsk som er relatert til bruk av data, handlinger som krenker rikets sikkerhet, jf. straffeloven §§ 90 og 91 osv. Problemstillingen gjelder også for rasistiske og hatefulle ytringer, jf. straffeloven § 135 a, men dette er spesielt dekket av mandatets tredje punkt, og skilt ut til særskilt behandling i kapittel 7.4.

Utvalget har som utgangspunkt avgrenset mot de nevnte problemstillinger. Det foreslås likevel noen presiseringer i slike straffebud der datavarianten har fremstått som særlig viktig eller praktisk.

I Datakrimutvalgets forrige utredning ble det opplyst at man ville komme tilbake til en ny behandling av gjennomføringen av datakrimkonvensjonen artikkel 9 om seksualiserte skildringer av barn, jf. NOU 2003: 27 kapittel 2.9.3 side 26. I lys av lovendringene på dette området som er beskrevet i kapittel 4.2.2, har utvalget valgt å avgrense mot denne problemstillingen. Utvalget ser det her som en fordel at reguleringen fremtrer som medienøytral. Det foreligger heller ikke spesielle samordningsbehov i forhold til annet regelverk som tilsier ny behandling av reglene.

Den nye problemstillingen som gjelder kriminalisering av handlinger som har til formål å oppnå møte med barn med tanke på seksuelt misbruk

(«grooming») er fremmet av regjeringen som egen lovsak (Ot.prp. nr. 18 (2006-2007)) og faller utenfor utvalgets arbeid. Utvalget bemerker imidlertid også her at det er naturlig at reguleringen er medienøytral.

### 4.3.3 Forholdet til spesiallovgivningen

Utgangspunktet har vært å avgrense mot bestemmelser i spesiallovgivningen. Verken mandatet eller utvalgets knappe tidsramme har gitt foranledning til å gjennomgå spesiallovgivningen med tanke på datakriminalitet. I visse tilfelle har det likevel ut fra en trusselorientert tilnærming vært naturlig å vurdere om enkelte bestemmelser i spesiallovgivningen bør flyttes til straffeloven, eller justeres i lys av Datakrimutvalgets forslag til straffebestemmelser. Spørsmålet har vært reist i forhold til masseutsendelse av elektroniske meldinger («spam»), som i dag reguleres av markedsføringsloven § 2 b. Forslag til ny markedsføringslov er sendt på høring, og § 2 b er foreslått videreført uten vesentlige endringer i utkast til ny markedsføringslov § 6-2. Utvalget foreslår å overføre første ledd av denne bestemmelsen i noe utvidet form til straffeloven, jf. utkastet § 14 (se kapittel 5.6.6).

Utvalget har også sett på forholdet mellom åndsverkloven §§ 53a og 53c og de korresponderende bestemmelsene i straffeloven. Problemstillingen er beskrevet i kapittel 5.1.2. Utvalget mener det er behov for samordning på grunn av det klare slektskapet mellom åndsverkloven § 53a, § 53c og straffeloven § 145 annet ledd, § 145b og § 262. Utvalget er klar over at enkelte av de endringer som ble foretatt i åndsverkloven i 2005, var gjenstand for en betydelig samfunnsdebatt og politiske overveielser. Dette gjaldt særlig åndsverkloven § 53a om beskyttelse av elektroniske sperrer. Imidlertid er de detaljerte folkerettslige forpliktelsene på dette området langt på vei styrende for den internrettslige gjennomføringen, med tilsvarende mangel på eget handlingsrom. Gjennomføringen kan dermed sies å få et visst teknisk preg. Det er også på det rene at forpliktelsen til å ha en regel som gjennomfører opphavsrettsdirektivet artikkel 6 om beskyttelse av elektroniske sperrer, kan dekkes i annen lovgivning enn den opphavsrettslige, for eksempel i straffeloven. Det vesentlige er regelens materielle innhold, ikke hvilken lov den er plassert i. Etter datakrimkonvensjonen artikkel 10 anses straffbare krenkelser av opphavs- og nærstående rettigheter som knytter seg til digitaliserte åndsverk, som datakriminalitet, noe som også tilsier harmonisering av bestemmelsene. Utvalget går enstemmig inn for harmonisering. Forslaget innebærer ikke noen materielle lovendringer. Utvalget har delt seg noe i synet på hvor omfattende harmoniseringsforslag som bør fremlegges i denne omgangen, se kapittel 5.1.2, og metodevalg ved gjennomføringen av harmoniseringen.

Ytterligere har utvalget avgrenset mot handlinger som innebærer krenkelse av straffeloven § 151 b. Bestemmelsen kom inn i straffeloven i forbindelse med datakrimutredningen i 1985, se kapittel 4.2.1. Bestemmelsen gjelder sabotasjehandlinger generelt, herunder sabotasje som rammer data og datasystemer, jf. uttrykkene «informasjonssamling» og «elektronisk kommunikasjon» i gjerningsbeskrivelsen. Bestemmelsen ble tatt inn i loven for å følge opp konvensjoner til bekjempelse av terrorisme som ble inngått på 1970-tallet. Det vises til merknadene om dette i NOU 1985: 31 «Datakriminalitet» side 32-33, og NOU 1993: 3 «Strafferettslige regler i terrorristbekjempelsen» side 8 kapittel 1.3 og side 44 kapittel 6.2.1. Det sentrale innhold i straffeloven § 151 b, er «volder omfattende forstyrrelse i den offentlige forvaltning eller i samfunnslivet for øvrig». Skadevoldende handlinger med slik omfattende virkning er i delutredning VII foreslått inntatt i ny straffelov kapittel 20 om vern av den offentlige ro og orden (se side 279 flg.). Utvalget antar at sabotasjebestemmelsen i sin helhet kan inntas i det nevnte kapittel slik kommisjonen foreslår, og finner det ikke naturlig å foreslå en spesialbestemmelse om datasabotasje. Derimot kan enkelte bestemmelser som er foreslått av utvalget tenkes anvendt i konkurrens med sabotasjebestemmelsen, noe avhengig av hvordan denne konkret utformes. Dette er særlig nærliggende for straffebudene om datamodifikasjon og driftshindring, jf. utkastet § 7 og § 13. Ved bruk av reglene om konkurrens kan man eventuelt få frem de sider ved sabotasjehandlingene som rammes av disse bestemmelsene.

Det kunne være ønskelig med en generell gjennomgang av reglene om hva det er adgang til å tilgjengeliggjøre på internett og hvilke regler som nærmere gjelder for dette. Problemstillingen gjelder både informasjon om andre (for eksempel bilder tatt med kamera på mobiltelefon) og informasjon om seg selv. Et eksempel på det siste kan være barn og ungdom som legger ut bilder av seg på internett. Spørsmålene reguleres i dag blant annet av personopplysningsloven (publisering av personopplysninger), åndsverkloven § 45c (publisering av fotografi) og av straf-

felovens bestemmelser om ærekrenkelse (§§ 246 flg.), forhånelse på grunn av tro (§ 142), diskriminerende eller hatefulle ytringer (§135 a) og bestemmelser til vern om privatlivets fred (§§ 390 og 390 a). Som utgangspunkt er det klart at reglene for tilgjengeliggjøring på internett bør være de samme som ellers i samfunnet, men det oppstår en rekke spørsmål som særlig skyldes at hvem som helst enkelt og kostnadsfritt kan foreta slik tilgjengeliggjøring. Blant annet har mange privatpersoner, også mindreårige, egne hjemmesider eller blogger. Utvalget har funnet å måtte avgrense også overfor disse problemstillingene i denne omgang.

Det har vært problemer forbundet med at noen registrerer domenenavn hvor andres firmanavn eller varemerke benyttes, eller andre navn eller betegnelser som er naturlig knyttet til andres virksomhet eller aktivitet. Det har imidlertid ikke vært mulig for utvalget å gå nærmere inn på slike forhold. For øvrig vises det også til enkelte avgrensninger som fremgår i kapittel 3.

### 4.3.4 Dataavlesing

Ifølge mandatet skal utvalget utrede og foreslå straffeprosessuelle regler om dataavlesing. Dataavlesing er et begrep uten entydig fastlagt innhold, og utvalget mener at det må utredes nærmere hva metoden består i. Metodebruken har dog vært berørt av Politimetodeutvalget som beskrev problemstillingen og metoden på følgende måte, jf. NOU 2004: 6 kapittel 10.7.11 side 207:

> «Gjennom kommunikasjonskontroll får politiet også opplysninger som kommuniseres mellom datamaskiner, for eksempel e-postforsendelser. På grunn av bedre tilgang til krypteringsprogrammer gir kommunikasjonskontroll i dag mindre informasjon enn tidligere. De moderne krypteringsprogrammer er så kompliserte at meldingen ikke lar seg dekryptere. Eneste måte å få tak innholdet på er derfor før meldingen krypteres. Dette har ført til at det i dansk rett er åpnet for dataavlesning ved å installere et program i datamaskinen som sender opplysninger til politiet. Programmet installeres ved datainnbrudd, og gir politiet opplysninger både om hva som meddeles og hvilke internettadresser som oppsøkes.»

Som straffeprosessuelt spørsmål faller dataavlesing på siden av utredningsarbeidet for øvrig i denne fasen. På grunn av de knappe tidsrammer som har vært satt for arbeidet med de materielle straffebestemmelsene, og fordi dataavlesing bør behandles i sammenheng med andre metodespørsmål, har utvalget latt dette spørsmål utstå til det senere utredningsarbeid. Dette har skjedd i samråd med Justisdepartementet.

## 4.4 Folkerettslige forpliktelser

### 4.4.1 Innledning

Utvalget har påsett at forslaget til straffebud overholder de folkerettslige forpliktelsene på området. Utvalget har også vurdert behovet for lovendringer for at Norge skal kunne ratifisere tilleggsprotokollen om rasistiske og fremmedfiendtlige handlinger begått i et datasystem (ETS 189), jf. punkt fire i mandatet. Dette spørsmålet er behandlet i kapittel 7.

### 4.4.2 Datakrimkonvensjonen

Med hensyn til de gjeldende folkerettslige forpliktelsene står datakrimkonvensjonen (ETS 185) av 8. oktober 2001 sentralt. Norge ratifiserte den 30. juni 2006 og den trådte i kraft pr. 1. oktober 2006. Konvensjonen angir minimumsforpliktelser til partenes strafferettslige og straffeprosessuelle lovgivning om datakriminalitet og dataetterforsking, og gir bestemmelser om internasjonalt rettslig samarbeid. Konvensjonen skal supplere andre konvensjoner på kriminalitetsbekjempelsens område, jf. konvensjonen artikkel 39. Som nevnt var utredningen i NOU 2003: 27 begrenset til å påse overholdelse av konvensjonens minimumsforpliktelser. Dette ledet til at Norge i flere tilfelle anvendte retten til å avgi erklæringer, jf. artikkel 40, og i forhold til artikkel 6 ble det foretatt en reservasjon, jf. artikkel 42. Utvalget mener at det på flere områder kan være ønskelig å gå lenger i å oppstille et strafferettslig ansvar for handlinger som rammer eller misbruker dataressurser, enn det som følger som minimumskrav etter konvensjonen. Lovforslagets bestemmelser om elektronisk kartlegging (§ 2), ulovlig anbringelse av utstyr m.v. (§ 3), data- og informasjonstyveri (§§ 5 og 6), etterfølgende befatning med ulovlig tilegnet data og databasert informasjon (§ 9), masseutsendelse av elektroniske meldinger (§ 14) og identitetstyveri (§ 15), er slike som klart går ut over konvensjonens minstekrav. Et flertall går også inn for straffebud som dekker artikkel 6 i sin helhet, jf. utkastet §§ 10 og 11, slik at reservasjonen kan trekkes.

### 4.4.3 Andre folkerettslige forpliktelser med spesiell relevans for datakriminalitet

Også andre folkerettslige forpliktelser har direkte betydning for utformingen av straffebud til vern om data. Dette gjelder blant annet tilgangskontrolldirektivet (1998/84/EF) og tilgangskontrollkonvensjonen (178 ETS) som ligger til grunn for straffeloven § 262 om rettslig vern for kodete tjenester. Det samme gjelder det beslektede regelsettet i WIPO-traktatene og opphavsrettsdirektivet (se kapittel 4.2.1) som gjelder vern om tekniske beskyttelsessystemer for vernede verk, som ble implementert i åndsverkloven ved lov av 17. juni 2005 nr. 97. Også programvaredirektivet (1991/250/EØF) kan nevnes her. Direktivet ligger til grunn for de spesielle reglene til vern om dataprogrammer i åndsverkloven, herunder § 53c.

### 4.4.4 FN-konvensjonen mot korrupsjon

FN-konvensjonen mot korrupsjon av 31. oktober 2003 pålegger medlemsstatene å innta straffebestemmelser som rammer gjerningspersonens egen befatning med utbyttet av en straffbar handling, såkalte sikringshandlinger («self laundering»). Ved lovendring av 30. juni 2006 nr. 49 ble straffeloven § 317 supplert med et nytt annet ledd som rammer slike sikringshandlinger. Noen av utvalgets forslag til straffebud beskriver et straffbart utbytte i form av databasert informasjon eller data, jf. utkastet §§ 5 og 6. Dette har gitt foranledning til å vurdere om slikt utbytte dekkes av den generelle bestemmelsen om sikringshandlinger, eller om det er behov for et eget straffebud om dette. Utvalget har konkludert med at det er behov for et eget straffebud som rammer etterfølgende befatning med data og databasert informasjon, jf. utkastet § 9, se kapittel 5.5.3.

## 4.5 Rettspolitiske utgangspunkter

### 4.5.1 Reglenes formål

Det grunnleggende formålet med straff er å hindre uønsket atferd og å styre borgernes atferd i ønsket retning, jf. formuleringen i Ot.prp. nr. 90 (2003-2004) side 82 kapittel 7.1. For å bidra til å oppfylle formålet må reglene gi god informasjon til borgerne om hva som er straffbart. Utvalget har derfor lagt vekt på å utforme straffebudene så klart og enkelt som mulig. God språklig tilgjengelighet kan også tenkes å bidra til en viss normdannende effekt.

Straffebud om datakriminalitet må imidlertid forholde seg til den teknologi som anvendes og de sikkerhets- og sårbarhetsspørsmål som reiser seg i tilknytning til dette. Et vesentlig formål med reglene er at de kan verne om data og datasystemers pålitelighet og støtte sikker bruk av datatjenester. Utvalget har likevel så langt som mulig ønsket å unngå bruk av tekniske faguttrykk. Faglige krav til datasikkerhet m.v., er imidlertid trukket inn i overveielsene ved utformingen av straffebudene.

Et vesentlig hensyn har vært å imøtekomme den jevne borgers alminnelige behov for vern mot datakriminalitet. På grunn av datateknologiens store nytte og brede anvendelighet kommer alle borgere i berøring med databaserte tjenester. Samtidig er datakompetanse og kunnskap om beskyttelsestiltak svært ulikt fordelt. Det er neppe rimelig å ha en straffelovgivning som bare tilgodeser kompetente aktører med de beste forutsetninger for å ivareta datasikkerhetshensyn. Dermed ville en stor brukergruppe uten spesiell kompetanse bli stående med et mangelfullt vern.

Borgerne er dessuten i stor grad avhengig av profesjonelle tjenesteytere for å kunne sikre seg. Utvalget mener at ansvar for å tilrettelegge for sikker bruk av datatjenester og elektronisk kommunikasjon først og fremst bør påhvile de profesjonelle aktører. Utvalget slutter seg derfor ikke til det utgangspunkt som tas i utredningen i NOU 2006: 6 «Når sikkerheten er viktigst» side 108 om at det påhviler et eget ansvar for den enkelte bruker med hensyn til dette problemet.

Et viktig legislativt utgangspunkt ved lovrevisjonen av 1987 (jf. NOU 1985: 31 side 31) var at

> «det primært hviler på innehaveren av anlegget å sørge for beskyttelse mot innsyn fra uberettigete. Først når det er tatt rimelige foranstaltninger i så måte kan han kreve hjelp fra strafferettsapparatet.»

Kommentaren gjaldt den såkalte datainnbruddsbestemmelsen. Da lovgiver fjernet beskyttelsesvilkåret i datainnbruddsbestemmelsen i straffeloven § 145 annet ledd, ved lovendringen 8. april 2005 nr.16, fravek man også det prinsipielle utgangspunktet fra 1985-1987. Begrunnelsen var at det forelå et behov for økt vern om data og datasystemer, se Innst. O. nr. 53 (2004-2005). Utvalget slutter seg til denne endring i synet på når det er rimelig å søke hjelp fra rettsapparatet. Dermed økes også vernet for den alminnelige brukergruppe.

Videre bør vernet om data være på linje med vernet om fysiske gjenstander. Også dette bidrar til et økt vern om data og datasystemer. Utvalget antar at denne delen av begrunnelsen for det strafferettslige vernet har sammenheng med at krenkelser overfor data og databasert informasjon i rea-

liteten rammer formuesrettigheter som eiendomsrett, leie-, lisens- og opphavsrettigheter. Dette gjelder enten dataene forvaltes i privat eller offentlig sektor. Siden data, databasert informasjon og datasystemer har stor økonomisk betydning i vår tid synes det rimelig at vernet må være på linje med vernet for fysiske gjenstander.

En annen del av den legislative begrunnelsen gjelder at datasystemer forvalter interesser av ikke-økonomisk art, som også trenger et effektivt vern mot krenkelser. Dette gjelder særlig ulike aspekter av personvernet, herunder retten til en privat sfære og til å bli latt i fred. Disse interessene ivaretas ikke i tilstrekkelig grad av personopplysningslovens regler, som er begrenset til å omfatte «personopplysninger». Det er uklart hvor langt personopplysningsbegrepet rekker og det straffe-rettslige vernet bør omfatte private data uansett om de er omfattet av begrepet eller ei.

Lovforslaget er ment å dekke praktiske tilfeller av straffverdig atferd knyttet til bruk av datateknologi. Datakriminalitet er noe som mange deler av rettsapparatet får befatning med og må ha evne til å håndtere. Dette gjelder hele kjeden bestående av etterforskere, påtalemyndighet, forsvarere og dommere. Enkle og oversiktlige straffebud som står samlet kan bidra til å effektivisere rettshåndhevelsen på dette feltet.

### 4.5.2 Nykriminalisering versus avkriminalisering

Borgernes respekt for straffelovgivningen tilsier at reglene ikke går lenger enn reelt begrunnet. I arbeidet med ny straffelov går man således inn for å fjerne straffebud som ikke lenger fremstår som relevante (avkriminalisering). På generelt grunnlag advares det også mot unødig nykriminalisering. Datakrimutvalget sier seg enig i dette som generell rettesnor for arbeidet. På den annen side gjelder lovforslaget om datakriminalitet livs- og samfunnsområder som kjennetegnes ved at borgerne på kort tid har fått tilgang på et vell av dataprodukter og datatjenester, og at samfunnet har blitt sterkt avhengig av datateknologien. Utvalget har ikke sett det som tvilsomt at dagens regler om datakriminalitet er utilstrekkelige, og at det foreligger et reelt behov for nykriminalisering. Ikke minst gjelder dette tyveri av data og databasert informasjon samt etterfølgende befatning med slikt straffbart utbytte. Det har heller ikke vært grunnlag for å foreta avkriminalisering i forhold til gjeldende rett.

### 4.5.3 Skadefølgeprinsippet

Skadefølgeprinsippet står sentralt ved utformingen av straffebudene i den spesielle del i ny straffelov og innebærer som alminnelig utgangspunkt at bare handlinger som medfører skade eller fare for skade bør straffesanksjoneres, se Ot.prp. nr. 90 (2003-2004) kapittel 7.5.1 side 88 flg. Datakrimutvalget har lagt dette premisset til grunn ved utformingen av lovforslaget.

Det antas at et straffebud ivaretar skadefølgeprinsippet dersom det beskriver en ytre konstaterbar handling som krenker data- og informasjonssikkerhetshensyn. Slike handlinger vil også ramme datasystemenes pålitelighet se nedenfor.

I tillegg søker lovforslaget som nevnt å ivareta ulike økonomiske rettigheter i dataressursene, eventuelt interesser av annen art, det vil si hensynet til privatlivets fred m.v., se ovenfor. Det kan reises spørsmål ved hva som i slike tilfelle må kreves for å kunne tale om en skade i skadefølgeprinsippets forstand. Her kan man skille mellom handlinger rettet mot datasystem og mot data/databasert informasjon.

Når et datasystem krenkes, rammes også påliteligheten og det foreligger en skade. Når handlingen rammer data eller databasert informasjon kan man skille mellom konkret og hypotetisk skade avhengig av om den berettigede til dataene eller informasjonen er klar over det inntrufne eller ei. Dersom vedkommende vet at data eller informasjon er slettet, manipulert eller kommet på avveie, foreligger klart nok en skade. Dersom vedkommende ikke er klar over det som har skjedd, for eksempel fordi opplysningene har vært lagret hos tredjemann, kan det i noen tilfeller være mer uklart hvordan man skal karakterisere hendelsen. I enkelte slike tilfelle kan man tale om hypotetiske krenkelser rent subjektivt sett. Det er heller ikke nødvendig at datasystemet som sådan er krenket ved hendelsen, for eksempel dersom dataene er manipulert av en bruker som er berettiget til systemet hvor dataene har vært lagret.

I tilfeller hvor det er tale om eksponering av informasjon undergitt lovbestemt taushetsplikt, foreligger et rettsbrudd og det må anses å foreligge en skade. Det anses også ønskelig at straffelovgivningen behandler data og databasert informasjon som et gode i seg selv. Dette reflekterer den store verdi som data og databasert informasjon har i dagens samfunn, kommersielt, i forvaltningen og i privat sammenheng.

Utviklingen av nye nettbaserte datalagringstjenester tilsier også at det er behov for et styrket vern om data og databasert informasjon, uavhen-

gig av om den berettigede har registrert noen krenkelse eller ei. Årsaken er at den berettigede i slike tilfelle er henvist til å stole på at dataene virkelig er tilstrekkelig beskyttet hos tredjemann (tjenesteyter). Den berettigete er vanligvis uten mulighet til selv effektivt å kunne kontrollere dette.

Utvalget mener altså at skadefølgeprinsippet må anses oppfylt overfor handlinger som rammer data og databasert informasjon selv om den berettigede ikke er klar over hendelsen. En eventuell straffesak må i enkelte slike tilfelle forutsettes initiert av tredjemenn, for eksempel tjenesteyter selv eller en tilsynsmyndighet. Det finnes eksempler fra praksis på dette, for eksempel vedrørende spredning av kredittkortnumre og passordlister på internett hvor de som er berettiget til kredittkortnumrene eller passordene ikke er klar over det som foregår. Det vises til Sunde 2006 «Lov og rett i cyberspace» på side 83, som omtaler en slik sak fra Nedre Romerike tingrett (passorddommen av 25. november 2003), hvor ca. 650 000 passord var kommet på avveie fra en tjenestetilbyder. Videre omtales en amerikansk sak hvor 19 personer ble tiltalt for spredning av kredittkortnumre fra et nettsted som het shadowcrew.com.

### 4.5.4 Hensynet til læring, forskning og kreativitet

Det er viktig at straffelovgivningen ikke er til hinder for læring, forskning og kreativitet på datateknologiens område. Et datamaskinprogram har et selvstendig rettslig vern som litterært åndsverk, jf. åndsverkloven § 1, og loven oppstiller begrensninger i adgangen til å foreta kopiering og dekompilering, jf. åndsverkloven §§ 39h og 39i. Åndsverklovens bestemmelser verner dataprogrammets konkrete utforming, det vil si konkrete funksjoner og virkemåte. De ideer og prinsipper som programmet er bygget på er ikke vernet. Tvert imot er det ansett å være i samfunnets interesse at man fritt kan analysere slike ideer og prinsipper. Derfor er det sentralt at straffebudene ikke griper inn i retten til å analysere og foreta omvendt utvikling av dataprogram i større utstrekning enn det som følger av åndsverkloven.

Alt i alt stiller dette lovgiver overfor en utfordring med hensyn til å komme frem til en passende balanse mellom et rettslig vern som sikrer at datasystemer nyter den tillit som skal til for å oppfylle viktige og nødvendige funksjoner i samfunnet, samtidig som det gis tilstrekkelig rom for aktiviteter som kan gi teknisk nyvinning.

I strafferettslig sammenheng aktualiseres interesseavveiningen først og fremst i tilknytning til utforming av vernet om tilgangskoder, og ved spørsmålet om det skal være adgang til å utvikle og anvende verktøy som kan benyttes til å skade eller trenge inn i datasystemer (for eksempel såkalte «exploits»). Dette er behandlet i kapittel 5.7 og gjennomført i utkastet §§ 10-12. Lovforslaget innebærer ingen innskrenkning i retten til å analysere de ideer og prinsipper som ligger bak programutvikling og ferdigstilte dataprogrammer og rammer ikke virkeområdet for åndsverkloven §§ 39h og 39i.

### 4.5.5 Andre hensyn

Til slutt presiseres det at straffelovgivningen bør være på linje med straffelovgivning i andre land det er naturlig å sammenligne seg med. En viktig grunn er at avvikende lovgivning kan medføre risiko for at Norge blir en «safe haven» for datakriminelle. Via globale elektroniske nettverk kan norske datatjenester utnyttes av kriminelle i utlandet dersom straffelovgivningen ikke er adekvat. Et eksempel er datamaskiner som misbrukes som anonymiserende mellomstasjoner i en straffbar handling som eventuelt materialiserer seg i et tredjeland. Dette harmoniseringshensynet er særlig ivaretatt ved gjennomføringen av datakrimkonvensjonen i norsk rett.

## 4.6 Hensynet til datasystemers pålitelighet

### 4.6.1 Pålitelighet

Det er en forutsetning for et velfungerende og utviklingsdyktig høyteknologisk samfunn at borgerne har tillit til at databaserte tjenester er sikre og virker som de skal. Denne tilliten bygger på at datasystemene kan anses å være pålitelige. På teknologisk nivå gjelder en rekke krav som må være oppfylt for at datasystemer skal kunne anses som sikre. De sentrale hensyn er kravene til konfidensialitet, integritet og tilgjengelighet. I nettbasert samhandling som er det praktiske i dag, har også krav til uavviselighet og autentisering fått økt betydning. Det vises til neste kapittel om disse hensynene.

Straffebud til vern av data, databasert informasjon og datasystemer må forholde seg til gjeldende standarder og tekniske konsepter for å oppnå datasikkerhet. Datakriminalitet vil ofte bestå i krenkelse av datasikkerhetshensynene og det er naturlig med et sammenfall i synet på hva som er en krenkelse av sikkerhetstiltak og hva som er straffbart. De underliggende hensyn er langt på vei de samme.

Dette er likevel bare et utgangspunkt. Siden straff er samfunnets strengeste sanksjon mot uønskede handlinger, krever utformingen av straffebud særskilte overveielser. Ifølge skadefølgeprinsippet må det fremstå som klart at handlingen er krenkende. Dertil må bruk av straff fremstå som rimelig.

Flere typer regelsett inneholder regler for organisering og behandling av data. Pliktene kan være straffesanksjonerte. Slike regler tar i stor grad sikte på å regulere informasjonssikkerheten for nærmere spesifiserte opplysninger. I den grad det er tale om databasert behandling av opplysninger er overholdelse av datasikkerhetstiltak viktig for å ivareta informasjonssikkerheten. De foreslåtte straffebud ivaretar datasikkerheten og følgelig informasjonssikkerheten på en klarere måte enn tidligere. Dette følger især av begrepsbruk og systematikk ved regelutformingen.

### 4.6.2 Datasikkerhetshensynene

*Konfidensialitet*

Konfidensialitet innebærer at data ikke blir gjort tilgjengelig for andre enn den berettigete. Data kan skjermes både ved fysiske og logiske tiltak. Fysisk skjerming kan for eksempel bestå i separering av nett, gjerne slik at man i en bedrift har et lukket nett til intern kommunikasjon og et annet nett ut mot internett. Innelåsing av fysiske lagringsmedier er et annet eksempel på fysisk skjerming. Logisk skjerming er databaserte tiltak for å beskytte mot adgang til data, for eksempel bruk av innholdskryptering, tilgangskontroll og brannmur. Også oppdateringsrutiner for å avbøte sårbarheter er tiltak som skjermer mot uberettiget tilgang til datasystemer.

I dagligtale benyttes ordet konfidensialitet ofte synonymt med hemmelig. Forslaget til straffebud om datakriminalitet inneholder imidlertid ingen forutsetning om at den databaserte informasjonen er hemmelig. Konfidensialitetskravet innebærer at den ansvarlige sørger for at data oppbevares eller behandles slik at det ikke er tvilsomt om adgang for andre er berettiget eller ei. Etter lovforslaget har det ikke betydning for skyldspørsmålet om informasjonen er hemmelig, taushetsbelagt eller lignende. Derimot kan slike omstendigheter være skjerpende momenter ved straffutmålingen, eventuelt lede til at lovbruddet anses å være grovt, jf. utkastet § 18.

Beslutning om skjermingstiltak treffes av eieren av datasystemet eller den som er berettiget til dataene. Utgangspunktet er at skjermingstiltak skal respekteres av brukerne av systemet. For å oppnå en klar grenseoppgang i forhold til andre bestemmelser, er bare skjerming etablert ved bruk av datainfrastruktur og logiske skjermingstiltak rettslig relevante i forhold til datakrimbestemmelsene. Med datainfrastruktur menes «datasystem» og «elektronisk kommunikasjonsnett», se utkastet § 1 bokstav a og e.

Skjermingstiltak er imidlertid ikke direkte tillagt rettslig betydning etter ordlyden i de foreslåtte straffebud. Spesielt vises det til utkastet § 4 om ulovlig tilgang til datasystem, som ikke anvender noe vilkår om beskyttelsesbrudd. Dette er i samsvar med straffeloven § 145 annet ledd, men ikke med straffeloven § 262 annet ledd og åndsverkloven § 53a første ledd, som gjelder bekyttelsesbrudd på tilgangskontrollerte tjenester og verk. Men vanligvis vil datasystemer, dvs. også slike som ikke behandler vernede tjenester eller verk, være beskyttet med tilgangskontroll og andre skjermingstiltak. Det betyr at en praktisk måte å overtre utkastet § 4 på er ved å bryte eller omgå en beskyttelse, for eksempel ved misbruk av et passord (passordinnbrudd). Metodebruken er mer utførlig beskrevet i kapittel 3.4.1.

Bruk av skjermingstiltak kan influere på rettsstridsvurderingen, særlig den subjektive side av handlingen. Det kan jo tenkes at gjerningspersonen ikke forsto at han var uberettiget til å skaffe seg tilgang til et datasystem nettopp fordi det ikke var skjermet. I så fall er ikke det subjektive vilkår for straff oppfylt. Motsatt vil en som har overvunnet skjermingsmekanismer på systemet vanskeligere kunne høres med at vedkommende ikke var klar over at tilgangen var uberettiget.

Krenkelse av alminnelige fysiske tiltak, slik som fysisk avstengning eller innelåsing, er ikke relevant i forhold til datakrimbestemmelsene. Handlinger som krenker slike tiltak må eventuelt rammes av de vanlige bestemmelsene om innbrudd og skadeverk. Slike straffebud kan anvendes i realkonkurrens dersom det i tillegg – etter innbruddet – foretas ulovlig tilgang på datasystemet eller uberettiget bruk av dette, jf. utkastet §§ 4 og 8. Dette innebærer en klargjøring i forhold til dagens rettstilstand vedrørende problemer i grenseflaten mellom straffeloven § 145 annet ledd og straffeloven § 147 (se Sunde 2006 «Lov og rett i cyberspace» side 140-141).

Lovforslaget inneholder straffebud som verner mot konfidensialitetskrenkelser, se utkastet § 4 om ulovlig tilgang til datasystem, og utkastet §§ 5 og 6 om informasjons- og datatyveri og utkastet § 9 om etterfølgende befatning med slik informasjon. Alle former for uberettiget tilegnelse og viderespredning anses følgelig som konfidensialitetskrenkel-

ser. I tillegg vises det til utkastet §§ 2, 3 og 10 som blant annet rammer uberettiget tilegnelse av opplysninger som kan anvendes for å begå konfidensialitetskrenkelser m.v.

### *Integritet*

Integritet betyr at noe er intakt. Begrepet kan også forstås som et krav til at data skal være opprinnelige, originale eller autentiske. Integritetshensynet innebærer et krav om at data ikke blir uberettiget endret (modifisert). Handlinger som tar sikte på å skade og slette datafiler er i kjerneområdet for krenkelser av integritetshensynet. Det samme gjelder tilføyelse av data som medfører at man ikke lenger kan stole på datasystemet, for eksempel tilføyelse av trojaner som utløser feilfunksjoner på systemet, fordi den også inneholder en såkalt «logisk bombe». Både kodetillegget representert ved trojaneren og feilfunksjonene er integritetskrenkelser fordi innhold og funksjonalitet er ulovlig endret. Også annen type kodetillegg, som for eksempel legger seg på datasystemet på grunn av et datavirus, innebærer en uautorisert endring og er en integritetskrenkelse.

Begrepet «data» foreslås definert etter generelle tekniske kriterier, jf. legaldefinisjonen i utkastet § 1 bokstav c. Det strafferettslige vernet gjelder dermed uavhengig av det innhold (informasjon) dataene bærer. Integritetsvernet gjelder således både på filnivå og systemnivå. En uberettiget endring i en datafil er et direkte integritetsbrudd på filen. Dersom funksjonaliteten på systemet er avhengig av innholdet i filen, for eksempel fordi det er en programfil, vil endringen ha betydning for datasystemet som sådan, dvs. for systemintegriteten.

Visse integritetsbrudd, for eksempel det å legge til adgangsrettigheter for tredjepersoner, eller å legge inn bakdører som åpner opp systemet for utenforstående, er filendringer med konsekvenser for systemsikkerheten. Til illustrasjon kan det vises til Rt. 2004 side 1619 (Bakdør-kjennelsen) hvor gjerningspersonene ved uberettigede endringer i passordfilen la til nye brukere. I tillegg foretok de modifikasjoner i systemoppsettet ved å legge til trojanere som fungerte som «bakdører». Handlingene ble bedømt som skadeverk, jf. straffeloven § 291. Etter utvalgets lovforslag rammes slike handlinger som datamodifikasjon, jf. utkastet § 7. Se også beskrivelsen i kapittel 3.4.3 og 3.4.4.

Utgangspunktet er at eieren av datasystemet har rett til å bestemme hvem som skal benytte det og til å sette regler for bruken. Brudd på slike regler vil lett innebære krenkelser av integritetshensynet. Integritetshensynet gjør seg gjeldende i åpne så vel som lukkede elektroniske kommunikasjonsnett og datasystemer. Selv om dataressurser kan sies å ligge åpent tilgjengelig, for eksempel på internett, gjelder normalt visse rammer for bruken. Det gis for eksempel adgang til å lese informasjon, men ikke til å endre data, for eksempel i en offentlig tilgjengelig rutetabell på internett. Uberettiget endring i en slik datafil er følgelig et integritetsbrudd selv om informasjonen er lagt fritt tilgjengelig for publikum.

Lovutkastet § 7 (datamodifikasjon) og § 12 (selvspredende dataprogram) er direkte begrunnet i integritetshensynet. Utkastet § 11 om ulovlig befatning med skadelig dataprogram, rammer utvikling, anskaffelse og spredning av dataprogram som er særlig egnet til å begå krenkelser av datasikkerheten, herunder integritetskrenkelser.

### *Tilgjengelighet*

Kravet til tilgjengelighet innebærer at datatjenester er tilgjengelige når og slik de skal for de berettigete. Kravet refererer seg både til funksjonalitet og kapasitet. Datasystemer skal ha en viss yteevne. Det er for eksempel sentralt for en bedrift at regnskaps- og administrasjonssystemer er løpende tilgjengelige. Tilsvarende må tjenestesteder på internett være tilgjengelige for brukerne. Tilgjengelighet er et rent funksjonskrav som oppnås ved mange forskjellige tiltak, for eksempel tilstrekkelig lagringskapasitet, båndbredde, oppdateringsrutiner, tiltak for datasupport eller nødaggregat i tilfelle strømstans. Når tjenesten er avskåret eller vesentlig forringet for eieren eller den berettigede bruker, foreligger tjenestenekt.

Siden handlinger som rammer tilgjengeligheten kan skje både ved å ramme fysiske installasjoner og datasystemets logiske funksjoner, oppstår behovet for en avgrensning av straffebudenes rekkevidde. Som nevnt avgrenses datakriminalitet mot rent fysiske handlinger. Lovforslaget retter seg derfor mot logiske krenkelser av tilgjengeligheten. Et klart tilfelle av logisk krenkelse av tilgjengeligheten er et tjenestenektangrep, også kalt «DoS-angrep», se kapittel 3.4.9. Dette er en form for overbelastningsangrep som har som mål å sette den angrepne server ut av funksjon. Når serveren slutter å fungere er tilgjengelighetskravet krenket i en slik grad at man taler om tjenestenekt. Skaden er midlertidig slik at driften kan gjenopptas når angrepet er over. Straffebestemmelsen i utkastet § 13 om driftshindring tar sikte på å ramme denne type krenkelse, se kapittel 5.6.4.

Også utestenging rammer tilgjengeligheten. Utestenging skjer ved at gjerningspersonen endrer påloggingsprosedyre eller passord slik at den berettigete ikke får adgang til datasystemet eller brukerkontoen. Fremgangsmåten innebærer at det er foretatt uberettiget endring i de datafiler som styrer tilgangsprosedyren, noe som er en integritetskrenkelse. I tillegg rammes tilgjengeligheten. Utkastet inneholder ikke noen bestemmelse som retter seg spesielt mot utestenging. Hovedsynspunktet er at handlingen rammes av bestemmelsen om datamodifikasjon, jf. utkastet § 7, siden integritetsbruddet er det primære ved selve handlingen. Krenkelsen av tilgjengeligheten er i tilfelle en konsekvens av integritetskrenkelsen og har betydning både for straffutmålingen og for om handlingen skal anses som grov, jf. utkastet § 18.

Også andre handlemåter kan gå ut over tilgjengeligheten i en slik grad at det er naturlig å reagere med straff. Dette kan for eksempel være tilfellet hvor en person setter i gang så krevende prosesser på et system at det går ut over øvrige brukeres normale utnyttelse. Når iverksettelse av slike prosesser skjer uten gyldig tillatelse, kan forringelsen av tilgjengeligheten for øvrige brukere tilsi at man står overfor et tilfelle av ulovlig bruk som kan rammes etter utkastet § 8 om uberettiget bruk av datasystem.

### *Autentisering – uavviselighet*

Autentisering er krav om sikkerhet for opprinnelse eller identitet. Autentiseringsprosedyrer kan sikre at bare den berettigete får tilgang til et datasystem, eller til en brukerkonto på et system. Slike prosedyrer kan også sikre at bare rette innehaver belaster et betalingskort, og bare berettigete datamaskiner får koble seg opp i et datasystem, eller får adgang til å spille av (lese) data fra spesielle tjenester eller lagringsmedier. Autentiseringstiltak kan altså gjelde både mennesker og datautstyr.

Tiltak for å sikre autentisering baserer seg på noe som den autoriserte bruker er, har eller vet, det vil si egenskap, objekt eller informasjon. Biometri baserer seg på egenskaper ved brukeren (noe han er). Objektbasert autentisering kan gå ut på bruk av nøkkelkort og dongler (noe han har). Kunnskapsbaserte autentiseringsmetoder kan kreve bruk av faste passord, pinkoder, eventuelt andre tilgangskoder (noe han vet). Samtlige teknikker har sine svakheter, så de benyttes ofte i kombinasjon for å øke sikkerhetsnivået. Krav om å trekke adgangskort i en kortleser og taste pinkode er en vanlig kombinasjon. Autentiseringshensynet begrunner derfor et særlig vern om tilgangskoder siden dette er et sentralt element i sikkerhetsløsningen.

Misbruk av tilgangskoder inngår som ledd i forøvelsen av en rekke databaserte lovbrudd. Ved bruk av stjålet tilgangskode kan man skaffe seg adgang til datasystem (ulovlig tilgang), belaste et kredittkort (kredittkortbedrageri), skaffe seg tilgangskontrollerte ytelser over nett (åndsverkloven § 53a, jf. § 2 siste ledd, og straffeloven § 262 annet ledd). For å bidra til å skape den nødvendige sikkerhet for fortsatt god utvikling av e-handel, antas det å være behov for straffebud som slår ned på forskjellige former for kodemisbruk. I tillegg er det et minimumsvilkår i datakrimkonvensjonen artikkel 6, at uberettiget spredning av tilgangskoder skal straffes som særskilt handling. Dette følger i dag av straffeloven § 145b, § 262 første ledd og åndsverkloven § 53a annet ledd og § 53c.

Utvalget har valgt å utforme straffebudene i lovforslaget slik at de retter seg mot selve resultatet av handlingen, det vil si den uberettigete tilgang eller tilegnelse, og har ikke oppstilt vilkår knyttet til hvordan handlingen skal skje annet enn at den må være uberettiget. Siden kodemisbruk hyppig vil være et ledd i handlingen slik den rent faktisk begås, bør også anskaffelse og fremstilling av kodene være straffbar. Det samme gjelder besittelse og spredning. Dette følger av utkastet §§ 3 og 10. Behovet for å styrke vernet om autentiseringsmekanismen er en vesentlig del av den legislative begrunnelsen. Autentiseringshensynet supplerer her de øvrige datasikkerhetshensynene.

Det er grunn til å understreke at uttrykket «tilgangskoder» har vid betydning. Det omfatter alle «opplysninger, databasert informasjon og data» som kan benyttes overfor tilgangskontrollen til et datasystem, eller til å anvende databaserte tjenester. Derfor omfattes mye mer enn koder som er implementert i selve datautstyret. For eksempel omfattes opplysninger om passord som gjerningspersonen uberettiget leser fra en «gul lapp». En tilgangskode kan altså være representert på annen måte enn i form av data eller databasert informasjon. Den behøver ikke bestå av en tegnstreng, som for eksempel en rekke numeriske tegn eller bokstaver. Dersom tilgangskoden er digitalisert, det vil si lesbar for et datasystem, kan den for eksempel bestå av et hologram eller et fingeravtrykk som er lastet inn i en brikke som skal anvendes overfor tilgangskontrollen. Den digitale representasjonen er en tilgangskode som uberettiget kan tilegnes, for eksempel ved uberettiget kopiering («skimming»).

Krypteringsteknikker kan anvendes for å oppnå autentisering. Utveksling av hemmelige

koder innebærer en bekreftelse for identiteten til parten (noe han vet eller har). Det kan være tale både om symmetrisk og asymmetrisk kryptering (offentlig nøkkelkryptering (PKI)), se kapittel 3.2.5 og 3.4.7. Bruk av asymmetrisk kryptering inngår i elektronisk signatur, som er en sikkerhetsmekanisme som kan sikre både autentisering og uavviselighet. Uavviselighet er viktig for å skape sikkerhet i nettbaserte transaksjoner. Medkontrahenten påstår for eksempel å ha mottatt en varebestilling som den angivelige bestilleren nekter å ha foretatt. Medkontrahenten kan via bruk av elektronisk signatur skaffe seg verifikasjon for identitet og at bestillingen virkelig er foretatt. Uavviselighet kan ses som en funksjon av integritets- og autentiseringstiltak.

– Autentiseringshensynet tilsier at man slår ned på identitetstyveri som en selvstendig forbrytelse, se utkastet § 15. Dette rammes ikke klart av noen straffebestemmelse i dag, men kan etter omstendighetene for eksempel rammes av reglene om krenkelse av privatlivets fred, jf. straffeloven § 390a, dersom handlemåten innebærer misbruk av en annens identitet. Indirekte har identitetstyveri betydning for tilliten til datasystemer og til den informasjon som formidles over databaserte tjenester. Lovbrudd etter utkastet § 15 forutsetter ikke misbruk av tilgangskoder. Vern om autentiseringshensynet er også en del av lovgrunnen for utkastet § 16 om kontomisbruk, som ofte skjer ved misbruk av koder for sikker identifikasjon. Utkastet §§ 15 og 16 er nærmere begrunnet i kapittel 5.6.7 og 5.8.

### 4.6.3 Andre hensyn

Lovforslaget går lenger enn å foreslå straffebestemmelser som er direkte forankret i datasikkerhetshensynene. Dette gjelder for eksempel utkastet § 6 om datatyveri. Datatyveri forutsetter en forutgående adgang til dataene. Denne adgangen kan være berettiget eller uberettiget. Dersom adgangen er ulovlig, jf. utkastet § 4, foreligger krenkelse av konfidensialitet. Selve kopieringen av data («tyveriet» eller tilegnelsen) kan muligens anses som en integritetskrenkelse, fordi det er foretatt en ulovlig handling på systemet. Det sentrale ved bestemmelsen er imidlertid at det er behov for vern om data som objekt i seg selv, slik at vernet kommer på linje med det som gjelder for fysiske gjenstander.

Regelen om ulovlig bruk av datasystem, jf. utkastet § 8, er bare delvis begrunnet i hensynet til datasikkerheten. Det sentrale er vernet om eierens investering i datasystemet. Eieren har rett til å bestemme både hvem som skal benytte systemet og hva det skal brukes til. Et annet spørsmål er hvilke kontrolltiltak eieren kan utøve for å påse at bruken holder seg innenfor de rammer han har satt. Rekkevidden av kontrolladgangen reguleres blant annet av regler om privatlivets fred, f. eks. EMK artikkel 8, arbeidsrettslige regler om kontroll med arbeidstakernes databruk, personopplysningsforskriftens regler om bruk av logger m.v. Disse reglene er det ikke nødvendig å gå nærmere inn på her.

Etter utvalgets oppfatning er det tilstrekkelig begrunnelse for straff at det foreligger brudd på retningslinjer som er gyldig fastsatt og kommunisert til brukerne. Dette følger av eierrådigheten, som ligger til grunn for tilsvarende regler som rammer uberettiget bruk av løsøregjenstand, jf. straffeloven §§ 261 og 393. For fast eiendom gir dessuten bestemmelsen om uberettiget opphold i hus, jf. straffeloven § 395 en viss parallell. Ved rettsstridig bruk av datasystem er det unødvendig også å søke begrunnelse i datasikkerhetshensynene, selv om handlingen kan komme til å krenke disse. Det kan for eksempel skje hvis en bruker installerer og tar i bruk programvare som retningslinjene av sikkerhets- eller kapasitetsmessige årsaker har satt forbud mot.

# Kapittel 5
# Nærmere om problemstillinger i tilknytning til lovforslaget

## 5.1 Oversikt over lovforslaget

### 5.1.1 Hovedelementer i lovforslaget

Lovforslaget inneholder følgende hovedelementer:

- Legaldefinisjoner. Utkastet § 1.
- Straffebud som rammer handlinger som hyppig skjer i forkant av ulovlig tilgang eller andre krenkelser overfor datasystem eller databaserte tjenester. Handlingenes formål er gjerne å skape grunnlag for gjennomføring av den etterfølgende krenkelsen. Utkastet § 2 (elektronisk kartlegging av datasystemer) og § 3 (ulovlig anbringelse av utstyr m.v.).
- Straffebud som rammer uberettiget tilegnelse («tyveri») og etterfølgende bruk av databasert informasjon og data. Utkastet §§ 5, 6 og 9.
- Straffebud som rammer handlinger som krenker hensynene til datasystemers pålitelighet og til de økonomiske og samfunnsmessige interesser som er forbundet med datasystemer. Utkastet § 4 (ulovlig tilgang til datasystem), § 7 (datamodifikasjon), § 8 (uberettiget bruk av datasystem), § 13 (driftshindring), § 14 (masseutsendelse av elektroniske meldinger) og § 15 (identitetstyveri).
- Straffebud som rammer uberettiget befatning med tilgangsdata og skadelig dataprogram. Utkastet §§ 10-12.
- Straffebud om kontomisbruk. Utkastet § 16.
- Bestemmelse om når grov uaktsomhet som skyldform kan lede til straff. Utkastet § 17.
- Bestemmelser om lovbruddet skal anses som grovt eller lite. Utkastet §§ 18 og 19.
- Straffebud som plasseres i øvrige deler av ny straffelov:
  - En skisse til regler om elektronisk dokumentfalsk.
  - Bestemmelser til den alminnelige delen i ny straffelov: Bestemmelser om jurisdiksjon, rettighetstap og inndragning, jf. utkast til § 7, § 69, § 76 annet ledd og ny § 76a. Et mindretall presenterer forslag til bestemmelse om filtrering som ny § 76b.
  - I tillegg foreslås en endring i § 390a i straffeloven.

### 5.1.2 Harmoniseringsspørsmålet

Utvalget har identifisert et harmoniseringsbehov mellom åndsverkloven §§ 53a og 53c, straffeloven §§ 145 annet ledd og § 145b, og straffeloven § 262. Det anses ikke å være tvilsomt at det foreligger en nær sammenheng mellom disse bestemmelsene siden de alle gjelder uberettiget tilgang til data, og handlinger som tar sikte på å tilrettelegge for uberettiget tilgang til data.

Følgende av bestemmelsene gjelder uberettiget tilgang til data: Åndsverkloven § 53a første ledd, straffeloven § 145 annet ledd og § 262 annet ledd.

Følgende bestemmelser gjelder tilrettelegelse for uberettiget tilgang til data: Åndsverkloven § 53a annet ledd og § 53c, straffeloven § 145b og § 262 første ledd.

Begrunnelsen for samordning og harmonisering er særlig å gi et mer oversiktlig lovverk. Dette oppnås ved å påse at reglene om uberettiget tilgang til data gis lik strafferettslig behandling uansett hvilket innhold dataene bærer. Per i dag fremstår de ovennevnte regler og grensesnittet mellom dem som så uoversiktlige at de er vanskelige å praktisere. Folkerettslige forpliktelser synes ikke å være til hinder for å integrere reglene i åndsverkloven § 53a og § 53c i datakrimkapitlet i den nye straffeloven (se kapittel 4.3.3 og 4.4.3). Forpliktelsene oppfylles ved at loven har et straffesanksjonert forbud mot omgåelse av tekniske beskyttelsessystemer som også gjelder digitaliserte vernede verk. Det er ikke noen betingelse at disse reglene står i åndsverkloven.

Utvalget har imidlertid delt seg i synet på hvorvidt harmoniseringen mellom åndsverkloven og straffeloven bør gjennomføres allerede på det nåværende stadium og hvordan harmoniseringen eventuelt bør gjennomføres. Flertallet (Willassen, Sellæg, Gulbrandsen og Taraldset) går inn for å implementere det vesentlige innholdet i åndsverkloven § 53a og 53c i datakrimkapitlet i den nye straffeloven. Mindretallet (Christensen og Rønning) støtter harmonisering, men går inn for at den eksisterende plasseringen av bestemmelsene foreløpig beholdes i åndsverkloven. Begrunnelsene følger nedenfor.

*Flertallet* legger størst vekt på det ovennevnte behovet for samordning. Det vises til at samordningen ikke medfører noen materiell endring i gjeldende rett, men gir en gevinst ved å lette mulighetene for å praktisere reglene som vil bli mer oversiktlige og lettere å tilegne seg. Flertallet er klar over at åndsverkloven § 53a nylig ble vedtatt, etter omfattende debatt og grundig behandling i Stortinget, men siden samordningsforslaget ikke innebærer noen materiellrettslige endringer, antas ikke dette å være til hinder for å gå inn for samordning nå. Rettstilstanden for hva som omfattes av åndsverkslovens regler om den opphavsrettslige enerett, privatkopieringsretten eller bibliotekenes adgang til å skaffe seg åndsverk i digitalisert form, jf. åndsverkloven §§ 2, 12 og 16, påvirkes ikke av lovforslaget. Forslaget gjør heller ingen inngrep i retten til å kopiere eller analysere et dataprogram, jf. åndsverkloven §§ 39h og 39i. Alle disse reglene gjelder som før.

Det kan også nevnes at ulovlig spredning av vernede verk ved bruk av fildeling på internett ikke berøres av lovforslaget. Slike handlinger er klart straffbare brudd på eneretten til å foreta tilgjengeliggjøring til allmennheten, jf. åndsverkloven § 2, jf. § 54 første ledd bokstav a, og lovforslaget endrer ikke dette.

Flertallet viser også til at lovforslaget gir lovgiver stor frihet ved gjennomføringen. Siden lovforslaget bygger på generelle begreper som «data», «dataprogram», «databasert informasjon», «datasystem» og «elektronisk kommunikasjonsnett», har lovgiver mulighet til å la være å integrere åndsverkslovens bestemmelser, uten at det av den grunn er nødvendig å foreta noen endring i bestemmelsene i lovforslaget. Men det innebærer i så fall at straffebudene får en smalere og mindre praktisk rekkevidde enn flertallet går inn for.

Full harmonisering slik flertallet går inn for forutsetter imidlertid at utkastet § 11 gjennomføres. I forhold til denne bestemmelsen foreligger det dissens, se kapittel 5.7.5. Dersom § 11 ikke gjennomføres kan heller ikke åndsverkloven § 53a annet ledd og § 53c integreres i datakrimkapitlet. Åndsverkloven § 53a første ledd kan imidlertid uansett integreres på grunn av sammenhengen med utkastet §§ 4-6.

Dersom lovgiver helt velger å avstå fra å integrere åndsverklovens bestemmelser § 53a og § 53c i datakrimkapitlet, antar flertallet at heller ikke straffeloven § 262 bør integreres. Området for sistnevnte bestemmelse dekkes nemlig nærmest i sin helhet av åndsverkloven § 53a, jf. § 2 siste ledd. Det vises videre til sammenhengen mellom disse bestemmelsene og åndsverkloven § 45 og § 45a, som igjen henger sammen med straffeloven § 262. Det synes derfor uansett å være nødvendig med en samordning mellom straffeloven § 262 og åndsverkloven § 53a. Dette kan altså gjennomføres i datakrimkapitlet i den nye straffeloven slik flertallet anbefaler. Alternativet antas å være at temaet skilles ut til fullstendig separat behandling i en annen prosess.

*Mindretallet* viser til den nære og indre sammenheng mellom åndsverkloven § 53a og øvrige bestemmelser i loven. Etter mindretallets oppfatning kan ikke åndsverkloven § 53a uten videre oppheves uten at vesentlige sammenhenger mellom reglene i åndsverkloven går tapt. Mindretallet er videre av den oppfatning at pedagogiske hensyn trekker i retning av at åndsverkloven § 53a ikke bør flyttes ut av loven idet utflytting av en sentral bestemmelse lett kan føre til en uønsket reduksjon av muligheten til å holde den fulle oversikten over regelverket. Mindretallet viser også til at åndsverkloven § 53a nylig er vedtatt, etter omfattende debatt og grundig behandling i Stortinget. Mindretallet ser likevel behovet for å vurdere det nærmere forholdet mellom denne bestemmelsen og straffeloven, men forutsetter at dette vil bli gjort når Kultur- og kirkedepartementet senere skal revidere åndsverkloven, jf. den kommende revisjonen som varsles i Ot.prp. nr. 46 (2004-2005). Mindretallet viser endelig til at bestemmelsene i datakrimkapitlet i første rekke verner eierens data og datasystemer mot angrep utenfra. Et datasystem kan imidlertid inneholde data, herunder dataprogrammer, som eieren av systemet kun har en lisensiert bruksrett til. Lisensavtalen og lovgivningen, herunder for eksempel åndsverkloven § 53a første ledd, setter grenser for retten til å utnytte slike data og dataprogrammer. Blant annet vil det kunne være i strid med slike begrensninger å kopiere data fra gjerningspersonens eget datasystem eller bryte beskyttelsessystemer som er innebygd i dataprogrammer som er installert på gjerningspersonens datasystem. Mindretallet ser at utnyttelse i strid med dette fra eieren av datasystemet kan være i strid med ordlyden i blant annet § 4 og § 5 i lovutkastet slik flertallet synes å legge til grunn, men mener at det burde vært vurdert å få dette enda klarere frem i lovteksten i forbindelse med en harmonisering med de aktuelle bestemmelsene i åndsverkloven. Tiden har imidlertid ikke tillatt full utredning av dette.

I den videre utredningen er flertallets standpunkt lagt til grunn.

### 5.1.3 Forholdet til datakrimkonvensjonen m.v.

Det gis her en oversikt over lovforslagets dekning av de folkerettslige forpliktelser, først og fremst datakrimkonvensjonens krav, men også krav etter tilgangskontrollkonvensjonen, tilgangskontrolldirektivet, opphavsrettsdirektivet og programvaredirektivet. Disse folkerettslige instrumenter er nærmere omtalt i kapittel 4.4.3 med videre henvisninger. Oversikten tar utgangspunkt i rekkefølgen i bestemmelsene i datakrimkonvensjonen.

Om valg av skyldform kan det nevnes at forsett er tilstrekkelig for å oppfylle datakrimkonvensjonens krav, men at konvensjonen også i flere tilfeller gir mulighet for å kreve en eller annen form for hensikt. Utvalget har basert seg på hovedregelen i den nye straffeloven alminnelige del § 21, jf. § 22, det vil si forsett. I visse tilfeller er det åpnet for grov uaktsomhet som skyldform, jf. utkastet § 17. Skyldkravet kommenteres ikke nærmere i gjennomgangen i dette kapittel.

Artikkel 1: Definisjoner av datasystem og elektroniske data: Definisjonene dekkes av legaldefinisjonene i utkastet § 1 bokstav a, b, c og e. Det vises også til merknadene i kapittel 5.2.

Artikkel 2: Ulovlig tilgang: Dette dekkes av utkastet § 4 om ulovlig tilgang til datasystem. Etter konvensjonen er det valgfritt om man foruten vilkåret om «urettmessig tilgang» (jf. oversettelsen) vil anvende et beskyttelsesvilkår eller vilkår om at det er tale om uberettiget tilgang til et helt datasystem (og ikke bare til en del av dette). Utkastet § 4 beskriver en krenkelse på det laveste nivået i forhold til de muligheter konvensjonen gir, dvs. straff for ulovlig tilgang til datasystem med krav om forsett. Det kreves ikke beskyttelsesbrudd. Overtredelse er oppfylt også ved ulovlig tilgang til «del av et datasystem».

Utkastet § 4 dekker også opphavsrettsdirektivet artikkel 6, for så vidt gjelder omgåelse overfor et vernet verk som er elektronisk lagret. I dag dekkes dette av åndsverkloven § 53a første ledd i alternativet «omgå effektive tekniske beskyttelsessystemer [...] for å kontrollere eksemplarfremstilling [...] av et vernet verk».

Artikkel 3: Ulovlig oppfanging av data: Dette dekkes av utkastet §§ 5 og 6 om informasjons- og datatyveri. De nevnte bestemmelsene dekker uberettiget tilegnelse av databasert informasjon og data, enten de er lagret eller overføres (mellom datasystemer), herunder det å fange opp signaler som overføres innenfor ett og samme datasystem. Etter konvensjonen er det adgang til å begrense straffebudet til å gjelde overføring mellom datasystemer. Som nevnt går lovutkastet lenger enn dette.

Utkastet §§ 5 og 6 dekker også kravene i tilgangskontrollkonvensjonen, tilgangskontrolldirektivet og opphavsrettsdirektivet for så vidt gjelder uberettiget dekoding eller omgåelse av beskyttelse overfor overføring av vernede tjenester og verk, det vil si det området som i dag dekkes av straffeloven § 262 annet ledd, og åndsverkloven § 53a første ledd, jf. § 2 siste ledd, jf. § 54 første ledd bokstav b. I § 53a første ledd er det alternativet «omgå effektive tekniske beskyttelsessystemer [...] for å kontrollere tilgjengeliggjøring for allmennheten av et vernet verk» som dekkes av utkastet §§ 5 og 6.

Som det fremgår, supplerer utkastet §§ 5 og 6, utkastet § 4 i forhold til området for åndsverkloven § 53a. Mens §§ 5 og 6 rammer dekoding av data under overføring, rammer § 4 dekoding av data som er lagret. Det vises til underkapitlet Harmoniserings- og konkurransspørsmål i kapittel 5.5.2 for en nærmere redegjørelse om sammenhengen mellom bestemmelsene.

Artikkel 4 og 5: Disse bestemmelsene gjelder skadeverk utført ved inngrep i dataenes integritet og i driften av et datasystem. Disse handlingene dekkes av utkastet § 7 (datamodifikasjon) og § 13 (driftshindring). Utkastet § 7 dekker i utgangspunktet både artikkel 4 og 5, fordi den på samme måte som konvensjonsbestemmelsene beskriver integritetskrenkelser. Etter artikkel 5 er det i tillegg et vilkår at integritetskrenkelsen resulterer i driftshindring. Forsettlig driftshindring som følge av integritetskrenkelse kan rammes av utkastet § 13 annet ledd, se kapittel 5.6.4. Dessuten bidrar utkastet § 13 første ledd om overbelastningsangrep, også til å dekke ødeleggelsesalternativet i artikkel 5. Spredningsalternativet i utkastet § 12 om selvspredende dataprogram supplerer utkastet §§ 7 og 13 i dekningen av artikkel 4 og 5. Spredning av er en form for «tilførsel av data», jf. artikkel 5, og resulterer regulært i flere av de øvrige alternativene beskrevet i artikkel 4 og 5, som «slette», «fjerne» eller «endre» data.

Artikkel 6: Misbruk av innretninger og tilgangsdata: Bestemmelsen skiller mellom rettsstridig befatning med tilgangsdata, jf. artikkel 6 nr. 1, a, ii, og rettsstridig befatning med innretninger (dataprogram og utstyr) som kan benyttes til å begå overtredelse som beskrevet i artikkel 2-5, jf. artikkel 6 nr. 1, a, i.

Rettsstridig befatning med tilgangsdata er dekket i utkastet § 10. Lovforslaget legger opp til en videre kriminalisering enn nødvendig for å dekke minimumsforpliktelsen, som bare gjelder spredning av tilgangsdata. Dette er i dag kriminalisert, jf. straffeloven § 145b. Etter utkastet § 10 foreslås det

å straffe anskaffelse, innførsel, fremstilling, besittelse, markedsføring og tilgjengeliggjøring av tilgangsdata.

Slik utkastet § 10 foreslås å lyde, dekkes ikke bare området for datakrimkonvensjonen artikkel 6 nr. 1, a, ii, men også de folkerettslige forpliktelsene bak straffeloven § 262 første ledd, åndsverkloven § 53a annet ledd og § 53c når dekodingsinnretningen er en tilgangskode.

Rettsstridig befatning med innretninger som kan benyttes til å begå overtredelse av handlingene nevnt i artikkel 2-5, foreslås straffet, jf. utkastet § 11. Den foreslåtte bestemmelsen dekker som nevnt artikkel 6 nr. 1, a, i, og her gir datakrimkonvensjonen reservasjonsadgang, jf. artikkel 6 nr. 3. I utvalget foreligger dissens i spørsmålet om å foreslå § 11. Et flertall går inn for bestemmelsen.

Slik utkastet § 11 foreslås å lyde dekkes ikke bare området for datakrimkonvensjonen artikkel 6 nr. 1, a, i, men også de folkerettslige forpliktelsene bak straffeloven § 262 første ledd, åndsverkloven § 53a annet ledd og § 53c, når dekodingsinnretningen består i skadelig dataprogram eller teknisk utstyr. Det er et vilkår at dekodingsinnretningen kan benyttes til å begå datakriminalitet i form av overtredelse av utkastet §§ 4-8, 10 eller 13-14. Disse overtredelsene dekker handlingene beskrevet i datakrimkonvensjonen artikkel 2-5 og uberettiget dekoding av vernede tjenester, verk, og dataprogrammer. Utkastet § 11 gjennomfører altså reservasjonsløst de folkerettslige forpliktelser som følger av datakrimkonvensjonen, tilgangskontrollkonvensjonen, tilgangskontrolldirektivet, opphavsrettsdirektivet og programvaredirektivet.

Artikkel 7: Datarelatert falsk: I utgangspunktet er det avgrenset mot dokumentfalsk, jf. kapittel 4.3.2. Utvalget er enig i straffelovkommisjonens merknad om at falskreglene må dekke datatilfeller og sier seg enig i de vurderinger som det er redegjort for i delutredning VII side 375 flg. I NOU 2003: 27 «Lovtiltak mot datakriminalitet» konkluderte dessuten Datakrimutvalget med at dagens regler om dokumentfalsk var tilstrekkelige for å tilfredsstille den folkerettslige forpliktelsen, se side 22 flg. Det antas likevel å være behov for en viss regelutvikling på dette området og utvalget presenterer derfor en skisse til nye regler om elektronisk dokumentfalsk, se kapittel 5.9.

Artikkel 8: Datarelatert bedrageri: I NOU 2003: 27 konkluderte utvalget med at dagens regler om databedrageri i straffeloven § 270 første ledd nr. 2, er tilstrekkelige for å dekke den folkerettslige forpliktelsen. I denne utredningen foreslås likevel et nytt straffebud om kontomisbruk, jf. utkastet § 16, for å klargjøre hjemmelen for en rekke praktiske varianter av databedrageri. Det foreslås også en korresponderende endring i straffeloven § 270 første ledd nr. 2.

Artikkel 9: Straffbare handlinger knyttet til befatning med seksualiserte skildringer av barn: Dette har utvalget avgrenset mot, se begrunnelsen i kapittel 4.3.2.

Artikkel 10: Straffbare handlinger knyttet til opphavsrett og nærstående rettigheter: Norsk rett oppfyller kravene i de konvensjonene som er listet opp i denne artikkelen. Det vises til Datakrimutvalgets vurdering i NOU 2003: 27 side 26 flg. Lovforslaget integrerer reglene om uberettiget tilgang, herunder uberettiget tilegnelse av vernede tjenester og verk som overføres elektronisk, i utkastet §§ 4-6, og §§ 10-11. Det vises til de tidligere kommentarene om dette. Integreringen endrer ikke gjeldende rett. De folkerettslige forpliktelsene for opphavsrettigheter og nærstående rettigheter vil være dekket i samme grad som før.

Artikkel 11: Forsøk og medvirkning. Dette dekkes av ny straffelov §§ 15 og 16.

Artikkel 12: Juridiske personers ansvar: Dette er spørsmål om foretaksstraff. Det er lagt til grunn at alle straffebestemmelsene kan overtres etter dagens regler om foretaksstraff i straffeloven § 48a og § 48b. Disse reglene er videreført i ny straffelov §§ 27 og 28 og reiser neppe spesielle spørsmål i forbindelse med lovforslaget.

Artikkel 13: Straffesanksjoner og tiltak: Denne bestemmelsen stiller krav om reaksjonsform og nivået. Lovforslaget oppfyller utvilsomt de vilkår som stilles her. Dessuten suppleres reaksjonsformene nevnt i den nye straffeloven med noen presiseringer om inndragning i ny straffelov § 69 annet ledd, og § 76 annet ledd og en særregel for inndraging av konto på et datasystem i ny straffelov § 76a. Et mindretall foreslår også filtrering av tilgang til internettsteder, jf. utkastet til en ny bestemmelse i ny straffelov § 76b.

Artikkel 22: Jurisdiksjon: Forpliktelsen etter denne bestemmelsen er oppfylt, jf. straffeloven § 12. Det foreslås likevel et supplement til bestemmelsen i ny straffelov § 7.

Lovforslagets bestemmelser i utkastet §§ 2, 3, 8, 9, 14, 15 og 16 går ut over datakrimkonvensjonens krav, og er særlig begrunnet i behovet for å effektivisere vernet om datasikkerheten og å bringe vernet om data og databasert informasjon på linje med det som gjelder for fysiske gjenstander. I tillegg vernes hensyn til privatlivets fred og til den personlige integritet. De sistnevnte hensyn som gjør seg særlig gjeldende for utkastet §§ 14, 15 og 16.

Tilleggsprotokollens (ETS 189) krav er allerede dekket i gjeldende straffelov. Det vises til kapittel 7.4 om overveielser knyttet til rasistiske og hatefulle ytringer.

## 5.2 Begrepsbruk

### 5.2.1 Prinsipper for utforming av begrepene

*Teknologi- og innholdsnøytralitet*

Lovforslaget definerer følgende begreper, jf. utkastet § 1: «Datasystem», «dataprogram», «data», «databasert informasjon» og «elektronisk kommunikasjonsnett». I spesialmotivene er det redegjort for begrepenes innhold, se kapittel 9.1. I tillegg inneholder lovforslaget enda tre begrepsdefinisjoner, men disse er tatt direkte inn i det straffebud som benytter begrepet. Det vises til definisjonen av «selvspredende dataprogram», i utkastet § 12 tredje ledd, «uriktig identitet» i utkastet § 15 første ledd annet punktum og «konto» i utkastet § 16 annet ledd.

Grunnbegrepet «data» inngår i alle begrepene i utkastet § 1, som således får et visst preg av sirkeldefinisjon. Utvalget mener imidlertid at hver definisjon inneholder tilstrekkelig med ny informasjon til å tilføre begrepene en selvstendig betydning, slik at sirkelelementet ikke utgjør noe problem.

Straffebudene i lovforslaget baserer seg på prinsipper om *teknologi- og innholdsnøytralitet*. Spørsmål om hva slags type «IKT-system» det er tale om og hva slags innhold dataene har, er ikke relevante for reglenes anvendelsesområde. Straffebudene omfatter «IKT-systemer», uansett om teknologien gjelder tele-, IT- og media (herunder kringkasting). Det samme gjelder innholdet. Om innholdet består av tekst, lyd, bilde eller dataprogram, er uten betydning. Den viktigste legaldefinisjonen er «data», som de øvrige begrepene bygger på. Infrastrukturbegrepene i utkastet § 1 bokstav a (datasystem) og bokstav e (elektronisk kommunikasjonsnett) gjelder utstyr og teknologi som kan lagre, behandle eller overføre «data». Også definisjonene av «dataprogram» og «databasert informasjon» viser tilbake til begrepet «data».

Av hensyn til behovet for vern av informasjon som er lagret på en type medier som krever annet teknologisk avlesningsutstyr, er begrepet «data» definert noe videre enn bare til å omfatte elektroniske signaler. Det tenkes for eksempel på informasjon som er lagret på hullkort, glassplater (microfich) eller i integrerte kretser (brikker / «chips»). Slik informasjon er «data», jf. utkastet § 1 bokstav c annet punkt. Kriteriet er at informasjonen ikke er lesbar uten bruk av teknisk utstyr. Begrepsbruken er i samsvar med databegrepet i straffeloven § 145 annet ledd. Bestemmelsen omfatter uttrykkelig data som kan lagres elektronisk eller ved «andre tekniske hjelpemidler». Utvalget har ikke sett noen grunn til å innskrenke anvendelsesområdet for databegrepet i den nye straffeloven. Tvert imot synes det å være klart at også slik informasjon må ha strafferettslig vern mot uberettiget avlesning m.v. Slik beskyttelse oppnås gjennom den noe vide definisjonen av «data».

*Forpliktelsen etter datakrimkonvensjonen*

Som et utgangspunkt for utformingen av definisjoner for «data» og «datasystem», kan det vises til datakrimkonvensjonen artikkel 1 bokstav a og b som definerer «datasystem» (*computer system)* og «elektroniske data» (*computer data)*. Begrepene er omtalt i NOU 2003: 27 «Lovtiltak mot datakriminalitet» kapittel 4.1 side 10, hvorfra siteres:

> «Konvensjonen bruker «computer system» for å betegne en innretning som består av maskinvare og/eller programvare, beregnet på eller brukt til automatisk behandling av digitale data.
>
> Konvensjonens bruk av begrepet «any device» tyder på at konvensjonen tar høyde for de siste årenes tekniske utvikling som har resultert i en konvergens mellom det vi tradisjonelt kjenner som områdene for tele, IT og media. I henhold til konvensjonen antas det ikke å være avgjørende hvilken type innretning som behandler dataene. Utvalget legger derfor til grunn at begrepet «computer system» er ment å være teknologinøytralt. Dette medfører at det ikke er avgjørende for resultatet om innretningen er (en del av) et tradisjonelt datasystem eller en annen innretning som har tilsvarende funksjoner. Innretningen kan være frittstående eller knyttet sammen i nettverk. Det elektroniske kommunikasjonsnettet som binder innretningene sammen kan være jordbasert eller radiobasert. Teknologivalget vil ikke være avgjørende for hvorvidt innretningen er å betrakte som et «computer system».
>
> En slik forståelse er i tilfelle i tråd med forståelsen nasjonalt innenfor området for elektronisk kommunikasjon slik den fremstilles i Ot.prp. nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon. Utvalget finner det hensiktsmessig å legge til grunn en teknologinøytral forståelse av begrepet «computer system» og bruker i det følgende det norske begrepet «datasystem».
>
> [...]

Konvensjonens definisjon av «computer data» bygger på ISO-definisjonen av data. Konvensjonen bruker begrepet «computer data» for å klargjøre at alle data som behandles elektronisk eller i annen direkte prosesserbar form er omfattet.

ISO-definisjonen av data ligger også til grunn for den norske forståelsen av begrepet «data». Data i denne sammenhengen forstås vanligvis som en elektronisk representasjon av informasjon.

Utvalget legger i det følgende en vid forståelse av begrepet data til grunn, der det avgjørende er om informasjonen er egnet til elektronisk behandling. Teknologivalget innenfor området elektronisk kommunikasjon vil dermed ikke være avgjørende for om noe faller inn under betegnelsen «data».»

Sitatet fremholder at som følge av konvergensen mellom tele, IT og mediesektorene, er prinsippet om teknologinøytralitet viktig. Datakrimkonvensjonens definisjoner av «datasystem» og «data» er følgelig så vide at alle de nevnte sektorer, enhver distribusjonsform og alt elektronisk innhold som derigjennom formidles, omfattes av konvensjonens vern. Som nevnt er dette prinsippet fulgt i lovutkastet.

Det betyr også at karakteren av den underliggende interesse eller rettigheter i dataene ikke har betydning for begrepene i utkastet § 1. Slike interesser og rettigheter kan være av svært ulik art, som for eksempel hensynet til privatlivets fred, kommersielle interesser, opphavsrettslige rettigheter, samfunnmessige hensyn til sikker infrastruktur, sikker forvaltning og hensynet til rikets sikkerhet m.v. Det er ikke meningen at karakteren av den interesse eller rettighet som måtte være rammet ved overtredelse av et straffebud om datakriminalitet, skal ha betydning for straffeskylden. Derimot kan det ha betydning ved straffutmålingen.

### 5.2.2 Begrepshierarkiet

Begrepene fordeler seg på tre nivåer.

#### *«Datasystem» og «elektronisk kommunikasjonsnett»*

Det laveste nivået omfatter infrastruktur, nemlig utstyr som er nødvendig for å lagre, behandle eller overføre data. Begrepene «datasystem» og «elektronisk kommunikasjonsnett» gjelder infrastruktur, se utkastet § 1 bokstav a og e.

Etter utkastet § 1 bokstav a er et «datasystem» definert som

«Enhver innretning bestående av maskinvare og data som foretar behandling av data ved hjelp av dataprogram.»

Definisjonen av elektronisk kommunikasjonsnett i utkastet § 1 bokstav e er likelydende med definisjonen i ekomloven § 1-5 nr. 2:

«Elektronisk kommunikasjonsnett: System for elektronisk kommunikasjon der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende ustyr eller funksjoner inngår.»

Definisjonene gjelder komponenter som i praksis har et nært samvirke, hvor begge – som det vil fremgå – etter omstendighetene kan inngå som komponent i den annen.

En datamaskin som fungerer alene oppfyller vilkårene i definisjonen av datasystem. Det samme gjør en mobiltelefon. Man kan si at delbegrepet «system» i slike tilfeller beskriver det samspillet mellom maskin og programvare som innebærer at det kan foretas behandling av data ved hjelp av et dataprogram. Både datamaskinen og mobiltelefonen kan derfor blant annet være utsatt for uberettiget tilgang og bruk, jf. utkastet §§ 4 og 8 som begge benytter ordet «datasystem» om det vernede objekt.

Datasystemer kan være koblet sammen og dermed inngå som komponenter i et større datasystem. Eksempler på dette kan være to sammenkoblede datamaskiner i en husstand, en bærbar pc som kommuniserer med en mobiltelefon (for eksempel for å behandle e-post og tekstmeldinger) og alle terminalene og serverne som inngår i datasystemet til en bedrift. Når det opprettes forbindelse mellom de lokale datasystemene foregår en ressursutveksling i et samspill mellom enhetene. Totalt sett utgjør de dermed et «datasystem» hvor de samarbeider om å foreta behandling av data ved hjelp av dataprogram.

Den linje som opprettes for å skape en sammenkobling mellom komponenter i et datasystem er et «elektronisk kommunikasjonsnett», jf. utkastet § 1 bokstav e. Datamaskinene står da som «annet koplings- og dirigeringsutstyr» i nettet, jf. utkastet § 1 bokstav e. I et slikt tilfelle er det naturlig å tenke på nettet som en del av datasystemet. Dette er i samsvar med datakrimkonvensjonens definisjon av «datasystem» i artikkel 1 bokstav a, jf. omtalen av definisjonen sitert i kapittel 5.2.1. Her står det blant annet at

«Innretningen [datasystemet] kan være frittstående eller knyttet sammen i nettverk. Det elektroniske kommunikasjonsnettet som binder

innretningene sammen kan være jordbasert eller radiobasert.»

«Elektronisk kommunikasjonsnett» omfatter imidlertid også store nett som for eksempel Telenors landsdekkende telefonnett, radio- og kringkastingsnett og satellittnett. Disse nettene danner den infrastruktur som bærer internett. Når det er tale om store elektroniske kommunikasjonsnett rettes oppmerksomheten mot overføringsevnen og «nettet» er i sentrum for oppmerksomhet og tankegang. Imidlertid inngår «datasystemer» som komponenter i slike nett. Rutere, basestasjoner, radio- og kringkastingssendere er eksempler på dette.

Rutere er enkle datamaskiner som bidrar til å sluse elektronisk kommunikasjon til rett adressat. Basestasjoner er datamaskiner som står som punkter i mobilnettet og bidrar til å koble opp og formidle samtaler. Det samme gjelder radio- og kringkastingssendere. Det nevnte utstyret omfattes av uttrykket «annet koplings- og dirigeringsutstyr», jf. utkastet § 1 bokstav e, og av definisjonen i utkastet § 1 bokstav a om «datasystem».

Elektronisk kommunikasjonsnett avgrenses mot slike komponenter i datasystemet som tjener til transport av signaler mellom prosessor og periferienheter, for eksempel fra tastatur eller mus til prosessoren og fra denne til utskriftsmaskinen. Overføringen kan skje i kabel eller trådløst (radiobølger). Uansett anses dette etter definisjonene i utkastet § 1, som en del av datasystemets interne prosesser. Dette følger også av at tastatur, mus og utskriftsmaskin ikke selvstendig sett oppfyller de rettslige vilkår for å være et datasystem, siden de ikke alene kan behandle data ved hjelp av et dataprogram. Det samme gjelder lagringsenheter som harddisk, minnepinne (USB-enhet), cd-er og dvd-er.

Dersom en enhet er så avansert at den oppfyller alle vilkårene i utkastet § 1 bokstav a, er den imidlertid «datasystem». Hvilke enheter som på et gitt tidspunkt kan karakteriseres som «datasystem» er avhengig av den tekniske utforming, og per i dag kan vilkårene for eksempel være oppfylt for visse avanserte utskriftsmaskiner.

Denne avgrensningen har betydning for om en handling skal anses som ulovlig tilgang til et datasystem, jf. utkastet § 4, eller som avlytting eller tapping av data under overføring som i så fall rammes av utkastet §§ 5 og 6. Ulovlig tilgang er rettet mot et «datasystem», jf. utkastet § 4. Det å fange opp signaler som går over tastaturlinjen er dermed uberettiget tilgang. Avlytting og tapping er rettet mot trafikken på et elektronisk kommunikasjonsnett og rammes av utkastet §§ 5 og 6, som følge av at begrepene «databasert informasjon» og «data» omfatter data under overføring.

Begrepene «datasystem» og «elektronisk kommunikasjonsnett» har en funksjonell rolle som fremgår av sammenhengen i de respektive straffebud. Utkastet § 2 kan tjene som eksempel. Her beskriver «datasystem» det objekt som utsettes for elektronisk kartlegging (krenkelsen), mens «elektronisk kommunikasjonsnett» begrenser straffebudets rekkevidde ved å gjøre det klart at bare kartleggingsvirksomhet som skjer over nett rammes. Annen kartlegging ved hjelp av tekniske metoder, for eksempel ved bruk av et digitalt kamera, omfattes ikke av bestemmelsen.

### *«Data» og «dataprogram»*

Det mellomste nivået gjelder de elektroniske signalene som lagres, behandles eller overføres på eller ved hjelp av et datasystem eller via et elektronisk kommunikasjonsnett. Slike signaler er «data», jf. utkastet § 1 bokstav c. Teknisk sett går det en hovedsondring mellom data som er lagret (kalles gjerne informasjon) og data som overføres (kalles gjerne kommunikasjon). Straffeloven § 145 annet ledd anvender en slik sondring, jf. «data eller programutrustning som er lagret eller som overføres». Datadefinisjonen i utkastet § 1 bokstav c er supplert med ytterligere et alternativ, nemlig slike signaler som «behandles» av et datasystem. Formålet er å unngå tvil om at dynamiske data omfattes av straffebudene i lovforslaget. Språklig sett lyder det noe anstrengt å si at data som for eksempel utnyttes i en database (som i et internasjonalt bookingsystem for flybilletter) er data som er lagret. Det er mer nærliggende å anse slike data for å være under behandling. Reelle hensyn taler selvsagt for at den strafferettslige beskyttelsen skal være på linje med vernet for data som er lagret og som overføres, og dette følger nå uttrykkelig av datadefinisjonen.

Også «dataprogram» er et definert begrep, jf. utkastet § 1 bokstav b. Dataprogram er en spesiell kategori data, og begrepet er følgelig på samme nivå som databegrepet.

### *«Databasert informasjon»*

Det øverste nivået er informasjonsnivået, som er når mennesker gjør seg kjent med det databaserte innholdet. Begrepet er «databasert informasjon», jf. utkastet § 1 bokstav d. Data transformeres til databasert informasjon ved sansebruk, dvs. ved å lese, høre eller føle (gjelder blant annet visse data-

tjenester for blinde). Eksempler på databasert informasjon er en fjernsynssending, et skjermbilde på en datamaskin eller lyd som formidles i en telefonsamtale når innholdet oppfattes av et menneske.

### 5.2.3 Forholdet til ekomlovens definisjoner

Siden ekomloven med forskrifter er det førende regelverk for tekniske, kommersielle og samfunnsmessige rammevilkår på feltet har utvalget lagt vekt på å harmonisere definisjonene i lovforslaget med ekomlovens definisjoner, jf. ekomloven § 1-5. Som nevnt er ekomlovens definisjon av elektronisk kommunikasjonsnett tatt inn ordrett i den korresponderende definisjonen i lovforslaget, se ekomloven § 1-5 nr. 2, jf. utkastet § 1 bokstav e.

Det kan imidlertid være grunn til å fremheve at datakrimbestemmelsene i lovforslaget ikke opererer med noen forutsetning om at den elektroniske kommunikasjonstjeneste som måtte være mål eller middel for handlingen, ytes mot vederlag. Dette er en forskjell i forhold til ekomloven, som gjelder elektroniske kommunikasjonstjenester som «normalt ytes mot vederlag», jf. ekomloven § 1-5 nr. 4. Dette innebærer at straffebudene kan ha et videre anvendelsesområde enn det som ville vært tilfelle dersom ekomlovens begrepsbruk hadde vært lagt til grunn fullt ut. Straffebestemmelsene gir således vern for elektronisk kommunikasjon og elektroniske kommunikasjonstjenester som omfattes av ekomloven, men er ikke nødvendigvis begrenset til dette.

### 5.2.4 Plassering av legaldefinisjonene

Legaldefinisjonene er skrevet med tanke på straffebud mot datakriminalitet, og foreslås inntatt i begynnelsen av kapitlet «Vern av data, databasert informasjon og datasystemer», se utkastet § 1. Alternativet hadde vært å plassere legaldefinisjonene i den alminnelige del. Faren for utilsiktede virkninger taler mot en slik plassering. Det vises til kommentarene i kapittel 4.1.2 om dette.

## 5.3 Rettsstridsreservasjonen

### 5.3.1 Innledning

Med unntak for utkastet § 14 om masseutsendelse av elektroniske meldinger, inneholder alle straffebestemmelsene i lovforslaget en uttrykkelig rettsstridsreservasjon, jf. vilkåret «uberettiget». Dette er i samsvar med vanlig lovteknikk ved utforming av straffebud, og fortolkning av vilkåret må i utgangspunktet skje konkret for hver bestemmelse. Her behandles noen generelle problemstillinger om rettsstrid vedrørende datakriminalitet.

Begrepet «uberettiget» er et utslag av den mer generelle *rettsstridsreservasjonen*. Om dette begrepet, hva det innebærer, og spørsmålet om det bør lovfestes en generell rettsstridsreservasjon, vises det til tidligere utredninger vedrørende ny straffelov, se NOU 1983: 57 side 122 og 141-142, NOU 1992: 23 side 105-112, NOU 2002: 4 side 220-222, Ot.prp. nr. 90 (2003-2004) side 211-215 og Innst. O. nr. 72 (2004-2005) side 45-48.

Hva som anses som uberettiget, må avgjøres på bakgrunn av normer utenfor strafferetten, særlig vil spesiallovgivning, avtale, kutyme, retningslinjer, instrukser og lignende være av betydning.

På samme måte som for andre straffebestemmelser vil generelle straffrihetsregler kunne utelukke straffansvar, for eksempel samtykke og nødrett. Det vil noen ganger være skjønnsmessig om man sier at handlingen ikke er uberettiget eller om man sier at den er uberettiget, men ikke straffbar på grunn av at gjerningspersonen handlet i nødrett.

Det kan i mange tilfeller reises spørsmål om når det foreligger en gyldig avtale. Før installasjon av programmer må bruker for eksempel klikke på en knapp hvor vedkommende aksepterer leverandørens lisensvilkår. Her kan det for eksempel, som en del av omfattende avtalevilkår, være innbakt en klausul om at brukeren aksepterer at et «spionprogram» installeres og aktiviseres sammen med resten av programpakken. I utgangspunktet må slike spørsmål løses etter avtalerettslige regler. Utvalget går derfor ikke nærmere inn på denne problemstillingen.

Nedenfor drøftes noen problemstillinger om rettsstrid og datakriminalitet som kan fortjene særlig omtale.

### 5.3.2 Bruk av tjenester på internett

Datamaskiner plassert i nett står der fordi det er et behov for å kommunisere med omverdenen. En slik datamaskin kan selv ta initiativ og sende meldinger til andre maskiner, men den stiller seg også i posisjon til å motta kommunikasjon som rettes til den. Innehaveren kan søke å beskytte sitt system mot uønsket kontakt, for eksempel ved å sette opp en såkalt «brannmur» som har i oppgave å stenge ute all trafikk som man ikke uttrykkelig har tillatt. Man kan for eksempel beslutte at bare trafikk til hjemmesiden og til e-posttjenesten skal slippe igjennom og at alt annet skal avvises. Prinsippet som følges er da at «alt som ikke uttrykkelig er til-

latt er forbudt». Et slikt beskyttelsestiltak hindrer ikke at datasystemet kan bli oppsøkt med sikte på å finne ut hvilke tjenester som tilbys, eventuelt om det er mulig å utnytte andre tjenester enn de som godtas av brannmuren. Dersom brannmuren fungerer slik den skal blir kontakten avvist. Men den annen part kan forsøke å omgå sperrene som er satt for å komme inn på irregulær måte.

Eksemplet viser for det første at som følge av at datamaskinen er plassert i nett kan den kontaktes av omverdenen, og at slik kontakt i seg selv ikke kan hindres. For det annet viser det at omverdenen kan oppsøke datasystemet for å finne ut hvilke tjenester som tilbys. Videre kan omverdenen forsøke å utnytte tjenestene, dvs. skaffe seg tilgang til og utnytte datasystemet. En tjeneste er en ressurs på systemet. Systemet kan være satt opp slik at visse tjenester bare skal kunne utnyttes av innehaveren selv mens andre skal betjene omverdenen. Overfor omverdenen kan ressursene gå med til å tilby ulike tjenester som for eksempel en opplysningsdatabase, salg av film og musikk som leveres elektronisk, en tjeneste for en pratekanal eller andre møteplasser, fildeling osv. Utnyttelse av slike ressurser når de tilbys av innehaveren, er selvsagt helt legitim og lovlig. Dette er nettopp formålet med og gevinsten av å kunne utnytte tjenester i nett.

Et datasystem inneholder imidlertid også ressurser som gjerne er forbeholdt innehaveren selv, for eksempel lagringsplass, styrings- og kontrollfunksjoner. Kontakt fra omverdenen kan iblant være motivert av ønske om å skaffe seg tilgang til disse ressursene, for eksempel for å lagre egne datamengder, for å skaffe seg anonymitet, for å skape feilfunksjoner på datasystemet, for å lage et uautorisert nett m.v.

Spørsmålet som reiser seg er om det kan sies noe generelt om når kontakt med andre datasystemer er uberettiget. Utgangpunktet er at hvert straffebud må tolkes for seg. Her er det særlig sammenhengen mellom utkastet §§ 2, 4 og 8 som belyses. Disse bestemmelsene gjelder elektronisk kartlegging, ulovlig tilgang og uberettiget bruk av datasystem.

Spørsmålet om rettsstrid ble aktualisert ved lovendringen i 2005 da beskyttelsesvilkåret i straffeloven § 145 annet ledd ble fjernet. Dette skjedde ved behandlingen i Stortinget, til tross for at både Datakrimutvalget og departementet gikk inn for å beholde vilkåret inntil spørsmålet var nærmere utredet. Forarbeidene i NOU 2003: 27 side 14-15, Ot.prp. nr. 40 side 14-15 og Innst. O. nr. 53 (2004-2005) side 5, sier derfor svært lite om betydningen av å fjerne vilkåret, og hvilken betydning dette har i forhold til begrepet uberettiget, kan ikke ses kommentert.

Utvalget går inn for å videreføre et straffebud om ulovlig tilgang, jf. utkastet § 4, uten å oppstille noe vilkår om beskyttelsesbrudd. Det er særlig vist til den jevne borgers behov for strafferettslig vern mot uberettiget tilgang og at det generelt er ønskelig med et sterkere strafferettslig vern om data og datasystemer. Fjerningen av beskyttelsesvilkåret bidrar til dette, men ikke alene. I tillegg foreslås et straffebud som rammer elektronisk kartleggingsvirksomhet, jf. utkastet § 2.

Det kan være naturlig å legge til grunn at en datamaskin på internett ønsker kontakt med omverdenen. Ellers burde den vært tatt ut av nettet. Utgangspunktet bør derfor være at det er legitimt å kontakte en datamaskin på nettet for å se om den har ressurser å dele med omverdenen. Men siden aktørene på internett ikke kjenner hverandre («hele verden») er det også naturlig å tenke at det gjelder begrensninger for omverdenens bruk av ressurser. Dette kan sammenlignes med en landhandel i innehaverens hus, hvor butikken er i første etasje og innehaverens leilighet i annen etasje. Det er tillatt å oppsøke butikken for å handle, men selvsagt ikke å ta seg inn i leiligheten og gå av gårde med sølvtøyet.

Hvis dette overføres til internett bør det anses som legitimt å forespørre datasystemet om det tilbyr tjenester som vanligvis er tilgjengelig for allmennheten på porter som normalt er dedikert til dette. Derimot er det ikke legitimt å fremsette en forespørsel for å avdekke hvorvidt datasystemet har sårbarheter som kan misbrukes for inntrengning. Utvalget har derfor lagt til grunn at forespørsler fremsatt for å avdekke om datasystemet har sårbarheter er straffbart, jf. utkastet § 2.

En forespørsel som nevnt setter også i gang prosesser ved at det datasystem som blir oppsøkt må gi svar på om det tilbyr de etterspurte tjenester, og registrere henvendelsen i sikkerhetsloggen. Forespørselen leder altså til en viss «bruk» av datasystemet. Men dersom forespørselen er lovlig etter utkastet § 2 er heller ikke den nevnte bruken rettsstridig. Det blir følgelig heller ikke tale om noe straffansvar etter utkastet § 8.

Høyesterett har kommentert en lignende situasjon i den såkalte portskandommen (Rt. 1998 side 1971). Her var spørsmålet blant annet om det forelå rettsstridig bruk av et datasystem på internett som følge av påloggingsforsøk på kjente tjenester (i dette tilfellet såkalte gjestekonti), og som følge av portskanning på systemet. Flertallet uttalte på side 1978-1979 at

> «Hvorvidt det kan anses som bruk av en løsøregjenstand å forespørre en datamaskin som er tilkoblet Internett om hvilke opplysninger den har å tilby, tar jeg ikke stilling til. Etter min oppfatning kan dette under enhver omstendighet ikke anses som uberettiget bruk [...]. Etter min oppfatning må den som har koblet sin datamaskin til Internett, og har valgt å la den svare på forespørsler, anses å ha gjort maskinen til en del av det informasjonssystem som Internett representerer. Ved å koble maskinen til Internett har datamaskineieren akseptert at det blir rettet forespørsler til maskinen om hvilken informasjon den har å tilby, og den aktivitet som skjer når maskinen svarer på slike forespørsler, kan da etter mitt syn ikke anses som uberettiget bruk av maskinen.»

Denne uttalelsen går noe lenger i å godta henvendelser over internett enn lovforslaget legger opp til. Mens Høyesterett godtok portskanning generelt, blir dette i utgangspunktet å anse som ulovlig kartleggingsvirksomhet, jf. utkastet § 2. Unntak gjelder eksempelvis dersom det dreier seg om å søke etter port 80 på det man på forhånd vet er en webserver. Da søkes det nettopp på en alminnelig tjeneste på en server som er dedikert til dette. Derimot er det ikke akseptabelt å foreta breddeskanning rettet mot port 80, for å teste om datasystemet kjører en gitt versjon av et operativsystem som gir mulighet for sårbarhetsinnbrudd. Slik kartleggingsvirksomhet anses å være «uberettiget» og straffbar.

Et annet tilfelle hvor løsningen også fremstår som temmelig utvilsom er at et datasystem har et brukergrensesnitt hvor det gis uttrykkelig anvisning på hvilke ressurser som tilbys og hvordan man skal kunne få tilgang til dem. Da er det disse retningslinjene som gjelder. En bruker kan ikke velge å skaffe seg tilgang på annet vis, for eksempel ved et sårbarhetsinnbrudd, selv om formålet er å få tilgang på de samme ressursene. Slik tilgang anses å være rettsstridig og straffbar. Og det fremstår også som nokså åpenbart at omverdenen ikke kan utnytte et datasystem med en berettiget forventning om å ha rettigheter som administrator på systemet. Utgangspunktet er at innehaveren av datasystemet ønsker å ha kontroll med det. Handlinger som retter seg mot kontroll og styringsfunksjoner rammer systemintegriteten. Det klare utgangspunkt og hovedregel er derfor at en slik handling må anses å være rettstridig.

### 5.3.3 Utlån av egne brukerrettigheter og passord

Problemstillingen gjelder om det kan sies noe generelt om når det er berettiget eller uberettiget å stille sine egne brukerrettigheter og passord til disposisjon for andre. Slike handlinger reiser spørsmål om straffansvar både for den som yter og for den som mottar og eventuelt anvender rettighetene. Langt på vei gjelder spørsmålet i hvilken grad samtykke kan frita for straffansvar for overtredelse av utkastet § 4 om uberettiget tilgang til datasystem og § 10 om uberettiget befatning med tilgangskoder. Det forutsettes at det ikke er tale om disposisjoner over egne brukerrettigheter på et datasystem man selv er innehaver av. I et slikt tilfelle står man fritt til å disponere over tilgangsrettighetene og ressursene.

Utgangspunktet er at eieren av et datasystem kan bestemme regler for bruken, herunder hvem som skal være berettiget til å bruke det. Eieren står dermed fritt til å gi brukerrettigheter til systemet. Spørsmål oppstår når en som er tildelt personlige brukerrettigheter til datasystemet samtykker til at en tredjeperson benytter datasystemet. Tredjeperson kan settes i stand til å bruke systemet ved at den berettigete bruker har gitt vedkommende opplysning om brukernavn og passord, eller ved å bli gitt tilgang rent fysisk etter at den berettigete bruker selv har sørget for påloggingen. I det siste tilfellet gis tilgangen uten at tredjeperson har fått opplysning om tilgangsdataene.

I utgangspunktet avhenger rettsstriden av utlånet av brukerrettighetene av rettsforholdet mellom eieren av datasystemet og innehaveren av brukerrettighetene, og dette må vurderes konkret. Mer generelt er det vanlig at innehaveren av et datasystem, for eksempel arbeidsgiver, har gitt retningslinjer om at brukerrettighetene er personlige og at passordet skal oppbevares hemmelig. Dette er også i samsvar med internasjonal og norsk standard for systemsikkerhet, jf. NS-ISO/IEC 17799:2005 Informasjonsteknologi, Sikkerhetsteknikk, Administrasjon av informasjonssikkerhet, kapittel 11, særlig 11.2.3 og 11.3. Det å gi passordet videre til uvedkommende i et slikt tilfelle må anses som klart rettsstridig, og er en overtredelse av tilgjengeliggjøringsalternativet i utkastet § 10.

Men også uten eksplisitt retningslinje som nevnt, er det nærliggende å anse spredningen som rettsstridig. Årsaken er innehaverens beskyttelsesbehov. De personlige brukerrettighetene gis normalt i en relasjon basert på tillit og lojalitet. Ofte vil brukerkontoen gi tilgang til ressurser som kun er ment for datasystemets brukere, typisk de ansatte, men som ikke er ment for omverdenen. Ut ifra slike omstendigheter alene kan eksponeringen av passordet anses som et tillitsbrudd og være rettsstridig. Dessuten må et passord holdes hemmelig for å oppfylle formålet. Når det er gitt videre, må

det erstattes med et nytt for at datasystemet skal være beskyttet. Dette støtter ytterligere at eksponering av passord er en rettsstridig handling. I motsatt retning kan det trekke at tilgangsdataene eventuelt bare ga mulighet for tilgang til brukerens egne data og ikke til de fellesresurser som tilbys samtlige ansatte (fellesressursene krever for eksempel et annet passord). Men ihvertfall i arbeidsforhold er det tvilsomt om dette kan lede til at handlingen ikke anses rettsstridig, siden det da normalt er arbeidsrelaterte data på det personlige brukerområdet. Slike data kan være sensitive og taushetsbelagte, men også uten slike restriksjoner er de normalt ikke ment for omverdenen. Hovedsynspunktet er altså at det å gi passordet videre er rettsstridig og rammes av utkastet § 10.

Spørsmålet er om også mottakeren kan rammes for å ha anskaffet passordet, jf. utkastet § 10. Rent objektivt er det tilfelle dersom det først var rettsstridig å spre det. Straffansvaret vil avhenge av det subjektive, dvs. om det forelå forsett eller grov uaktsomhet, jf. ny straffelov § 21 og utkastet § 17. Selve den omstendighet at det gjelder et arbeidsrelatert passord vil være et tungtveiende moment for at det foreligger grov uaktsomhet.

Et annet spørsmål er om selve det å gi tilgang til en annens system, og å benytte det, uten at passordet er eksponert, er rettsstridig. Her kan det oppstå spørsmål om ansvar for ulovlig tilgang, jf. utkastet § 4. Det forutsettes at det ikke er tale om samtidig å begå en overtredelse av utkastet §§ 5 og 6, fordi rettsstriden da vil være klar.

Det kan neppe sies noe helt generelt om dette, annet enn at dersom det foreligger retningslinjer, skal de følges. Uten retningslinjer må spørsmålet løses konkret og resultatets rimelighet må gis stor vekt. Blant de momenter som vil ha betydning er hvor kontrollert omstendighetene rundt tilgangen er. Dersom brukerkontoens innehaver for eksempel står ved siden av og følger med på at bedriftsrelaterte data ikke blir eksponert, er heller ikke lojaliteten til datasystemets eier nødvendigvis brutt. Motsatt dersom kontoens innehaver overlater databruken til tredjeperson uten å følge med, eventuelt også over et ikke ubetydelig tidsrom. Videre vil graden av sensitivitet av de data som behandles på systemet, virksomhetens art og alminnelig praksis i virksomheten for bruk av datasystemet, ha betydning.

I et tilfelle som nevnt er innehaveren av brukerkontoen medvirkende til at hovedmannen (tredjeperson) uberettiget skaffer seg tilgang til datasystemet. Medvirkeren vil normalt ha oversikt over de lokale regler for databruken, mens det ikke nødvendigvis er tilfelle for tredjepersonen. De subjektive vilkår må vurderes individuelt. I dette tilfellet er det bare aktuelt med ansvar for forsettlig forhold, jf. ny straffelov § 21. Det er nærliggende å anta at dette kan lede til at vilkårene for straff er oppfylt for medvirkeren, men ikke for hovedmannen.

Et annet spørsmål er hvorvidt det er straffbart å benytte et datasystem, når bruken kun skjer fordi det faktisk var adgang til det. Problemstillingen gjelder bare bruk av datamaskin som er fysisk tilgjengelig, ikke utnyttelse over nett som er behandlet i kapittel 5.3.2. Dataterminaler som åpenbart er satt opp som publikumstjenester, for eksempel i en hotellresepsjon, holdes utenfor. For å illustrere problemstillingen tenkes det for eksempel på at en uvedkommende benytter en personlig arbeidsstasjon som står ledig. Det kan jo være tale om en dataterminal som står i et sentralbord og innen fysisk rekkevidde for besøkende. Det gjøres ikke noen forutsetning om at bruken i seg selv er ulovlig etter andre bestemmelser i datakrimkapitlet, for eksempel at det er tale om rettsstridig informasjonstilegnelse, jf. utkastet § 5. Det kan være tale om bruk av uskyldig karakter isolert sett, for eksempel at den uvedkommende bruker dataterminalen til å sjekke sin webbaserte e-postkonto.

Dette antas å måtte løses etter de samme retningslinjer som gjelder for utnyttelse av datasystemer over internett. Det må altså foretas en vurdering av situasjonen hvor spørsmålet er om datasystemet innbyr til slik bruk eller ikke. Svaret vil som regel være negativt, med mindre det som nevnt er tydelig at dataterminalen er ment for publikum. Som nevnt kreves det ikke anvendelse av konkrete beskyttelsestiltak for å ha strafferettslig beskyttelse for sitt datasystem. Utgangspunktet er således at tredjeperson må skaffe seg tillatelse til å utnytte datasystemet for at tilgangen skal være rettmessig. I fysiske omgivelser bør det ikke by på problemer å avklare hvorvidt man er berettiget til å skaffe seg adgang eller ei.

I tråd med dette fremstår det også som nokså utvilsomt at «slapp» omgang med passord ikke gir tredjeperson rett til å benytte slike passord. «Passordtyranniet» kan lede til at passord skrives ned for eksempel på gul lapp rett ved dataterminalen. Selv om det å lese et slikt passord ikke nødvendigvis vil anses som rettsstridig, fordi det lå i dagen slik at det i praksis var uunngåelig, gis ikke tredjeperson noen rett til å bruke passordet eller gi det videre. Begge de sistnevnte tilfellene vil være rettsstridige handlinger etter utkastet §§ 10 og 4.

### 5.3.4 Tilegnelse av digitaliserte vernede verk – åndsverkloven § 53a m.v.

Etter lovforslaget dekkes åndsverkloven § 53a første ledd av utkastet §§ 4-6. Åndsverkloven § 53a første ledd har en rettsstridsreservasjon i tredje ledd annet punktum som lyder:

> «Bestemmelsen i første ledd skal heller ikke være til hinder for privat brukers tilegnelse av lovlig anskaffet verk på det som i alminnelighet oppfattes som relevant avspillingsutstyr.»

Bestemmelsen skal leses i sammenheng med åndsverkloven § 12 siste ledd. § 12 omhandler privatkopieringsretten, og siste ledd lyder:

> «Det er ikke tillatt å fremstille eksemplar etter denne paragraf på grunnlag av en gjengivelse av verket i strid med § 2, eller på grunnlag av et eksemplar som har vært gjenstand for eller er resultat av en omgåelse av vernede tekniske beskyttelsessystemer, med mindre slik eksemplarfremstilling er nødvendig etter § 53a tredje ledd andre punktum.»

Bestemmelsen i åndsverkloven § 12 siste ledd stiller krav om lovlig kopieringsgrunnlag, dvs. at det ikke lovlig kan tas privat kopi av et eksemplar som enten har vært ulovlig tilgjengeliggjort eller som har vært krenket ved en omgåelseshandling som nevnt i § 53a første ledd, eller som er et resultat av en slik omgåelseshandling. Det sistnevnte alternativet tar sikte på tilfeller hvor tilegnelsen ikke lar seg se atskilt fra omgåelsen, noe som for eksempel er tilfelle for piratdekoding av fjernsynssignaler. Bestemmelsen gjør unntak for omgåelser som er nødvendig for å realisere privat bruk av verket.

Reglene innebærer således at det uansett er lov til å fremstille en kopi dersom det er nødvendig for å realisere den private bruken. Det er også tillatt å benytte denne kopien som grunnlag for privat kopiering etter § 12 første ledd. Som et eksempel kan forbrukeren altså rettmessig kopiere lydspor fra en beskyttet cd til mp3-spilleren, og benytte mp3-filen som lovlig kopieringsgrunnlag for privat kopiering, jf. § 12 første ledd.

Flertallet antar at denne rettstilstand ville være tilfelle også uten en uttrykkelig regel om det i § 53a tredje ledd, fordi det ikke kan anses som rettsstridig å foreta dekoding for privat utnyttelse av et lovlig ervervet verk. Dersom lovgiver finner å ville beholde bestemmelsen er det imidlertid mulig for eksempel å flytte den til åndsverkloven § 12, med en henvisning til §§ 4-6 i datakrimkapitlet i den nye straffeloven.

### 5.3.5 Nettvett

På internett utvikles det kutymer for kommunikasjon, og det antas at disse iblant kan ha relevans for innholdet i rettsstridsreservasjonen. Utviklingen av slike kutymer er med på å gi internett dets dynamiske karakter. Det innebærer at lovgivningen ofte vil komme til kort med mindre det legges inn et rom for skjønn som kan ta hensyn til praksis. Et grunnleggende vilkår er imidlertid at det er tale om en praksis som er god, eller i det minste ikke er skadelig, og som må anses som klar, festnet og velkjent for dem som berøres av den. Videre kan det være grunn til å ta hensyn til normer for anbefalt atferd som tar sikte på å skape et miljø for sikker sosial omgang på internett. Disse normene er i en annen posisjon enn en kutyme, fordi normene i motsetning til kutymen, ikke nødvendigvis er nedfelt i en eksisterende praksis, men tilstreber å danne en ønsket praksis. Normene tillegges altså en selvstendig betydning for vurderingen av spørsmålet om rettsstrid.

Et aktuelt eksempel gjelder bruken av pseudonymer på internett. Det gjelder i stor utstrekning kutyme for bruk av fiktiv identitet på internett. Hvorvidt dette er en god eller dårlig kutyme beror på sammenhengen, og her varierer det meget mellom tilfellene og hva som søkes oppnådd med å anvende pseudonymet. Det kan dreie seg om handlinger over et så vidt spekter som fremsettelse av en politisk ytring uten å risikere forfølgning for sitt synspunkt (sikre reell ytringsfrihet), barn og ungdoms bruk av uriktig identitet som et alminnelig tiltak for å sikre seg mot ubehagelig eller farlig kontakt, fremsettelse av straffbare ærekrenkelser uten å bli holdt til ansvar, eller voksne som søker kontakt med mindreårige under foregivende at man selv er en ungdom.

For å sikre økt grad av personvern, herunder begrense bruken av elektroniske spor, satses det stadig mer på å utvikle teknologi som sikrer pseudonymitet, dvs. at man generelt er anonym, men kan spores opp dersom det har et lovhjemlet formål, for eksempel å bekjempe kriminalitet. Slik teknologi kalles PET (etter engelsk «Privacy Enhancing Technologies»).

På dette feltet skjer det en stor utvikling av normer, sosial praksis og teknologi. I korthet kan disse momentene ha betydning for når en overtredelse av forbudet mot elektronisk identitetstyveri, jf. utkastet § 15, er å anse som rettsstridig. Som en generell rettesnor antas det at nettvettregler som utarbeides for å støtte barn og ungdoms bruk av internett på sikker måte, bør ha stor betydning for å fastlegge hva som er rettsstridig for så vidt gjel-

der bruk av fiktiv identitet, slik at straffebudene støtter opp om dette. Slike nettvettregler kan også gi grunnlag for slutninger om hva som anses som rettsstridig praksis, nemlig de handlinger som reglene tar sikte på å sikre overfor.

## 5.4 Handlinger som skaper stor fare for gjennomføring av andre former for datakriminalitet

### 5.4.1 Problemstilling

Utvalget mener det er behov for straffebud som klart rammer visse innledende handlinger som skaper særlig stor fare for at andre straffbare handlinger begås. Det er tale om elektronisk kartleggingsvirksomhet og ulovlig anbringelse av utstyr m.v. på eller i tilknytning til datasystem eller elektronisk kommunikasjonsnett.

### 5.4.2 Elektronisk kartlegging

Elektronisk kartlegging av datasystemer er en aktivitet som går ut på å anvende dataprogrammer (kartleggingsprogrammer) over nett til å undersøke datasystemer. Slik kartlegging kan foregå på mange måter. Det vises til den generelle omtalen i kapittel 3.4.2. Formålet kan være å identifisere datasystemer som er sårbare for inntrengning eller misbruk. Aktiviteten kan også rette seg mot et spesifikt datasystem for å skaffe opplysninger om egenskaper og tjenester som er tilgjengelige på dette.

Rettspraksis har eksempler på begge former for kartleggingsvirksomhet. Det kan vises til bakdør-kjennelsen i Rt. 2004 side 1619, hvor aktiviteten gikk ut på å finne en mengde datamaskiner som var sårbare for en viss type angrep. På grunnlag av kartleggingen trengte gjerningspersonene seg inn i 437 servere i 33 land. I portskandommen (Rt. 1998 side 1971) og sms-dommen (Rt. 2004 side 94) foretok gjerningspersonene grundige undersøkelser mot datasystemer som var valgt ut på forhånd. Her gjaldt det altså kartleggingsvirksomhet som ble målrettet utført mot bestemt identifiserte datasystemer.

Elektronisk kartlegging er et regulært sikkerhetstiltak når det foretas av en som har i oppgave å ivareta sikkerheten på datasystemet. Kartleggingen kan for eksempel bidra til å avdekke tjenester som står tilgjengelige for omverdenen til tross for at de skulle vært stengt. På denne måten kan den ansvarlige skaffe opplysninger som er nødvendige for å kontrollere systemet.

Men elektronisk kartlegging er også en ordinær metode for å forberede en inntrengning i et datasystem. Gjennom kartleggingen registreres hvilke sårbarheter datasystemet har, og følgelig hvordan det kan misbrukes.

Lovligheten av elektronisk kartlegging i form av portskanning ble behandlet i den nevnte portskandommen. Spørsmålet var om handlingen ble rammet av straffeloven § 393 om ulovlig bruk av løsøregjenstand. Kartlegging innebærer nemlig kontakt med datasystemet, som sender tilbake elektroniske signaler («svar») på en forespørsel om egenskaper og tjenester er aktivisert på systemet. Responsen innebærer at prosesser iverksettes på det datasystem som er gjenstand for undersøkelsen. Slike prosesser kan karakteriseres som «bruk». Høyesteretts flertall kom til at kartleggingen ikke var å regne som *ulovlig* bruk da den fornærmede ved tilkoblingen til internett måtte anses å ha akseptert at datasystemet ble satt i virksomhet på grunn av slike aktiviteter.

Straffelovkommisjonen tar opp problemstillingen om portskanning bør være straffbart, se delutredning VII side 373 (spesialmerknader til § 30-14). I en kommentar til portskandommen bemerkes at det

> «ikke er åpenbart at grensen for det ulovlige bør gå der hvor Høyesterett har trukket den. En kartlegging av portene i et fremmed datasystem står sentralt ved forberedelse av datainnbrudd, og vil som regel gjøre det nødvendig for offeret å foreta nærmere undersøkelser. Det bør vurderes om en lovendring er nødvendig for å fange opp slik kartlegging.»

Utvalget utelukker ikke at fjerningen av beskyttelsesvilkåret i straffeloven § 145 annet ledd ved lovendringen i 2005, kan ha medført at elektronisk kartleggingsvirksomhet rammes av forbudet mot å skaffe seg adgang til data. Dette forutsetter at adgangen til de opplysninger på datasystemet som kan kartlegges, anses å være uberettiget. Det vises til drøftelsen i Sunde 2006 «Lov og rett i cyberspace» side 138-139 og side 148. Problemstillingen ble imidlertid ikke vurdert i forbindelse med lovbehandlingen, så rettstilstanden er neppe helt avklart.

I lys av disse omstendighetene antas det å være behov for en uttrykkelig avklaring av om elektronisk kartlegging skal være straffbar eller ei. Det er vanskelig å se at det foreligger aktverdige grunner for kartleggingsvirksomhet uten at det skjer etter ønske fra datasystemets eier. Elektronisk kartlegging er mer nærgående og dermed farligere, enn for eksempel det å foreta observasjoner av inn-

gangspartier og vinduer til et hus man ønsker å bryte seg inn i. Årsaken er at elektronisk kartlegging nødvendigvis forutsetter en kontakt med det datasystem som er gjenstand for observasjon. Kartleggingsprogramvare kan også bygges ut med exploits som automatisk utnytter sårbarheter som avdekkes. Det er altså kortere vei mellom kartlegging og misbruk enn ved observasjon i fysiske omgivelser. Dette gir datasystemets eier mindre mulighet for å skjerme seg.

Mot kriminalisering taler at elektronisk kartlegging kan være vanskelig å forfølge, både på grunn av utnyttelse av anonymiseringsteknikker og fordi saken ofte vil kreve etterforsking i utlandet. Bruk av ressurser på etterforsking kan være vanskelig å forsvare med mindre kartleggingen faktisk har resultert i andre straffbare handlinger. Dermed kan det sies å være mindre reelt behov for å ramme kartleggingsvirksomheten med straff. På den annen side er det liten grunn til å akseptere atferden og det antas at et straffebud kan ha en holdningsskapende effekt. Allmennpreventive hensyn gjør seg også gjeldende med styrke. Mye av kartleggingsvirksomheten kan forstås i lys av fraværet av et klart forbud, noe som har gitt et visst spillerom for en type nysgjerrighetsdrevet aktivitet som særlig var gjeldende i internetts barndom. I dag fremstår slik kartleggingsvirksomhet som lite legitim, og den registreres som «fiendtlige oppkall» av sensorer som fanger opp dette. Hensett til den preventive effekt et slikt straffebud vil ha, ikke bare for kartleggingsvirksomheten som sådan, men også for den datakriminalitet som utløses av opplysningene fra kartleggingen, foreslås det å kriminalisere uberettiget elektronisk kartlegging av datasystemer.

For så vidt angår portskanning gjør de hensyn som Høyesterett la vekt på i portskandommen seg fortsatt gjeldende. Utvalget mener imidlertid at disse hensynene ikke går så langt som Høyesterett trakk dem i den nevnte dommen. Men etter utvalgets syn bør det i hvert fall ikke anses som uberettiget å sjekke om et datasystem koblet til internett tilbyr tjenester som vanligvis er tilgjengelig for allmennheten på porter som normalt er dedikert til dette. Det må for eksempel være lovlig å sjekke om en datamaskin tilbyr en webserver, er vert for chatting eller tilbyr en åpen ftp-server på ordinær port. Det vises for øvrig til drøftelsen av rettsstridsreservasjonen i forbindelse med bruk av tjenester på internett i kapittel 5.3.2.

I spesielle tilfelle kan elektronisk kartlegging være så intens at den utgjør en belastning på datasystemet og går ut over dets funksjonsevne. Hvis kartleggingen på denne måten rammer tilgjengeligheten, utgjør den en form for tjenestenekt og kan rent objektivt rammes av forbudet mot driftshindring, jf. utkastet § 13. Dersom forsett om driftshindring mangler vil handlingen ikke kunne straffes etter denne bestemmelsen. Selve registreringen av egenskapene til datasystemet kan også etter ordlyden rammes av forbudet mot datatyveri, jf. utkastet § 5. Men handlingen er i periferien av hva bestemmelsen er ment å dekke, og det kan være grunnlag for en innskrenkende fortolkning på dette punkt. Utkastet § 4 om ulovlig tilgang til datasystem kommer ikke til anvendelse fordi kartleggingen ikke innebærer noen overskridelse av datasystemets grense, dvs. en «tilgang» til systemet som sådan. Kartleggingsaktivitet kan neppe heller rammes som forsøk på ulovlig tilgang, jf. utkastet § 4, jf. ny straffelov § 16, fordi handlingen i seg selv ikke innebærer noe inntrengningsforsøk, bare registrering av opplysninger.

Det antas følgelig å være behov for en særskilt bestemmelse om forbud mot elektronisk kartlegging av datasystem. Spørsmålet er hvordan et straffebud mot elektronisk kartlegging skal utformes slik at det blir tilstrekkelig presist og ikke får for stor slagvidde. Rent objektivt er det kun tale om å ramme kartleggingsaktivitet som skjer over det elektroniske kommunikasjonsnettet. Og det gjelder kun aktivitet rettet direkte mot det datasystem som kartlegges. Indirekte kartlegging, for eksempel ved bruk av databaser på internett som kan inneholde opplysninger om datasystemer og dets tjenester, omfattes ikke. Dette blir å sammenligne med konsultasjon i alminnelige oppslagsverk. Videre antas det å være nødvendig å oppstille et vilkår knyttet til formålet med kartleggingen. Hensynet bak straffebudet er å virke preventivt overfor aktiviteter som kan gi grunnlag for andre straffbare handlinger overfor datasystemet. Det synes dermed naturlig å kreve at kartleggingen skjer med tanke på å avdekke sårbarheter. Dermed unngår man at straffebudet favner for vidt.

Straffebudet om elektronisk kartlegging er tatt inn i lovforslaget § 2. Det vises ellers til særmerknadene i kapittel 9.2.

### 5.4.3 Ulovlig anbringelse av utstyr

Utvalget mener det er behov for å ramme handlinger som går ut på å plassere utstyr eller programvare på eller i tilknytning til datasystem eller elektroniske kommunikasjonsnett for å skaffe seg informasjon man ikke er berettiget til. Dette bidrar til å effektivisere vernet om datasystemer, databaserte tjenester og informasjon. Noen eksempler kan klargjøre formålet med straffebudet:

*Pinkoder*

Det er velkjent at kriminelle plasserer utstyr på automater for å fange opp pinkoder, for eksempel videokamera i nærheten av en minibank eller en bensinpumpe hvor man kan benytte kontokort. En annen variant er bruk av såkalte «falske fronter» som festes på utsiden av slike automater for å registrere avtrykk av pinkoden når den tastes inn av brukeren.

Denne tilegnelsen av pinkoder kombineres ofte med tyveri av kortet. En metode er å sørge for at automaten tilsynelatende «sluker» kortet, som dermed gis opp som tapt av eieren. Etterpå fiskes kortet opp fra automaten av den kriminelle. Dette kalles «libanesisk slynge» («Lebanese loop»). En annen variant er ulovlig kopiering av kontoinformasjonen i magnetstripen på kortet, såkalt «skimming». Den kriminelle kan kombinere bruk av pinkode og stjålet kort eller kopiert magnetstripe og foreta uberettigete kontooverføringer og kontant- og vareuttak. Disse handlingene straffes som (data)bedrageri eller tyveri, se kapittel 3.5.4 flg. Men utplasseringen av utstyret for å skaffe pinkoden er etter dagens rettstilstand straffri. Utvalget foreslår altså å kriminalisere dette.

*Avlytting og tapping*

Et annet straffverdig tilfelle er å installere utstyr eller programvare for å foreta avlytting eller tapping av elektronisk kommunikasjon, eller lese innholdet på et datasystem, se kapittel 3.4.6.

Den uberettigete informasjonstilegnelsen rammes som informasjons- eller datatyveri, jf. utkastet §§ 5 og 6. Straffebudene verner data og databasert informasjon som er lagret og som overføres. Også forsøk på uberettiget tilegnelse vil være straffbart, jf. ny straffelov § 16. Selve plasseringen av utstyret m.v. rammes ikke av disse reglene.

*Gjeldende rett og begrunnelse for forslaget om et eget straffebud*

Etter gjeldende rett er de nevnte handlingene straffrie. Selve utplasseringen av utstyr innebærer ikke en overskridelse av grensen for straffbart forsøk, jf. straffeloven § 49 (ny straffelov § 16). Dersom gjerningspersonen for eksempel forbereder avlytting av en kommunikasjon han regner med at vil finne sted på lørdag, kan han straffritt montere utstyret på torsdag. Da er han bare i fasen for straffri forberedelse. Straffeloven § 145 a nr. 3 representerer et unntak ved at anbringelse av «lytteapparat, lydbånd eller annen teknisk innretning» i slikt øyemed er straffbart. Bestemmelsens rekkevidde er imidlertid begrenset og gjelder bare forberedelse til telefonavlytting (og romavlytting, som ikke omfattes av utvalgets forslag). Utplassering av utstyr for avlytting av elektronisk kommunikasjon, jf. straffeloven § 145 annet ledd, omfattes ikke av forbudet i straffeloven § 145 a nr. 3.

Det antas at straffeloven § 393 heller ikke gir tilstrekkelig hjemmel for straff i disse tilfellene. Bestemmelsen krever at det foreligger rettsstridig «bruk» av løsøregjenstand. Hvorvidt vilkåret er oppfylt beror på den fremgangsmåte som er valgt for den rettsstridige informasjonsinnhentingen. For det praktiske tilfelle at et kamera er montert i nærheten av minibanken for å filme tastetrykk, er straffeloven § 393 neppe anvendelig, siden dette ikke kan karakteriseres som «bruk» av minibanken. Montering av en «falsk front» på minibanken representerer formodentlig et grensetilfelle for hva som kan kalles «bruk». Hvis fremgangsmåten består i å installere en «nettverksniffer» på eget datasystem for å fange opp passord som sendes over nettverket, er man klart utenfor straffeloven § 393. Denne fremgangsmåten, som er meget praktisk, er nærmere behandlet nedenfor.

Utplassering av utstyr m.v. er nødvendig for gjennomføring av et planlagt straffbart foretagende som nevnt. Handlingen skaper usikkerhet ved bruk av databaserte tjenester og er klart straffverdig. På denne bakgrunn foreslås straffebudet i utkastet § 3.

Skjæringspunktet for fullbyrdet straffbar handling foreslås å gå ved selve utplasseringen av utstyret. Det spiller ingen rolle om lovovertrederen har aktivisert utstyret såfremt formålet er å foreta en tilegnelse som nevnt i utkastet § 3 første ledd bokstav a eller b. Selve tilegnelsen av data og databasert informasjon, herunder tilgangsdata, foreslås straffet som en egen handling, jf. utkastet §§ 5, 6 og 10. Dersom lovovertrederen har tatt i bruk utstyr som nevnt i utkastet § 3 og lykkes i å tilegne seg informasjon, vil utkastet § 3 kunne anvendes i konkurrens med utkastet §§ 5, 6 og 10. Men formålet med utkastet § 3 er først og fremst å gi grunnlag for å gripe inn på et tidligere stadium, før tilegnelsen har skjedd. I slike tilfelle blir det bare tale om straff for overtredelse av utkastet § 3.

Pinkoder m.v. som kan registreres ved kamerabruk eller «falske fronter» omfattes *ikke* av utkastet §§ 5 og 6. Grunnen er at opplysningene når de fanges opp ikke er data eller databasert informasjon, jf. begrepsbruken i utkastet § 1 bokstav c og d. Det er kun tale om opplysninger som anskaffes ved å studere inntastingen slik den lar seg observere på videoopptaket eller ved å undersøke avtrykkene avsatt på falsk tastatur. Slike opplysninger nyter

ikke noe generelt strafferettslig vern. Man kunne tenkt seg at skjæringspunktet for fullbyrdet handling gikk ved tilegnelsen av disse opplysningene. Men et slikt kriterium ville utløse en rekke spørsmål om når tilegnelsen skjedde. Det kan være ved filmopptaket, registreringen eller den senere tolkingen av informasjonen. I tillegg kommer de bevismessige problemer ved anvendelsen av en slik regel. Både rettstekniske og bevismessige hensyn taler dermed for at skjæringspunktet går ved den ytre konstaterbare handling, nemlig utplasseringen av utstyret. Det er også da sårbarheten for den databaserte tjenesten oppstår.

Utkastet § 3 rammer ikke bare utstyr og dataprogram som plasseres på andres systemer, men også om det plasseres på eget system. Forutsetningen er at formålet er å begå en handling som nevnt. Dette er praktisk med tanke på å ramme forberedelse til uberettiget avlytting av nettverkstrafikk. Elektronisk kommunikasjon kan sendes i form av pakker og hver enkelt av disse pakkene inneholder informasjon om hvilken adressat pakken (og følgelig kommunikasjonen) skal til. Ved ordinær overføring vil nettverkstrafikken passere de datamaskiner som er koblet til nettet, men maskinene vil ikke fange opp andre kommunikasjonspakker enn de som er adressert til dem. Det er imidlertid mulig å ta i bruk dataprogram som «fisker opp» elektronisk kommunikasjon som *ikke* er adressert til den datamaskin man anvender. Et slikt program kalles ofte en «sniffer», jf. beskrivelsen i 3.4.6. Selve *bruken* av programmet rammes av forbudet mot uberettiget tilegnelse av data, jf. utkastet § 6. Etter utkastet § 3 rammes *installeringen* av slik programvare.

I denne sammenheng må det anses å være uten betydning for straffverdigheten om anbringelsen av dataprogrammet skjer på egen eller en annens datamaskin. For gjerningspersonen vil det normalt være mest hensiktsmessig å gjøre det på egen maskin fordi han da har kontroll både på programvaren og de data som tilegnes. I et tilfelle hvor avlyttingsprogrammet er installert på en annens maskin – og dette er gjort uten tillatelse – innebærer handlingen også en overtredelse av utkastet § 7 om datamodifikasjon.

Som det fremgår rammer utkastet § 3 utplassering både av fysisk utstyr og programvare. Dette er et utslag av prinsippet om teknologinøytralitet. Straffbarheten av en handling bør ikke avhenge av hvilken teknologi som konkret er benyttet, men formålet med handlingen. En tastetrykksregistrator som registrerer de signaler som sendes til datamaskinen fra tastaturet, kan enten være en fysisk gjenstand på tastaturkabelen eller programvare som er installert i det datasystem som utsettes for krenkelsen. I begge tilfelle kan de loggede tastetrykkene sendes automatisk til et program på gjerningspersonens datamaskin, men det er også mulig for gjerningspersonen å hente dem fysisk. Dette siste alternativet er kanskje det mest sannsynlige hendelsesforløp når registratoren er en fysisk gjenstand. Plasseringen av tastetrykksregistratoren rammes av utkastet § 3 i begge tilfellene, mens bruken rammes av utkastet §§ 5 og 6.

## 5.5 Strafferettslig vern for data og databasert informasjon

### 5.5.1 Rettspolitiske uttalelser m.v.

Mens vernet om eiendomsretten har vært regnet som tilstrekkelig grunn for straff, når krenkelsen gjelder fysiske formuesgoder, har ikke dette kommet tilsvarende til uttrykk for data. Det vises blant annet til bestemmelsene om underslag og tyveri, som retter seg mot uberettiget tilegnelse av (løsøre) gjenstand, jf. straffeloven §§ 255 og 257. Det er alminnelig antatt at disse bestemmelsene ikke kommer til anvendelse på uberettiget tilegnelse av data.

Oslo tingretts dom av 10. mars 2005 (TOSLO-2004-84792) er et utslag av denne rettsoppfatningen. En ledende ansatt i et telemarketingselskap var i ferd med å gå over i stilling som administrerende direktør i et konkurrerende selskap. Før han sa opp stillingen i telemarketingselskapet kopierte han innholdet på den såkalte «produksjonsserveren» til 5-7 cd-er som han tok med seg ut av bedriften. Det var tale om ca. 23 000 datafiler. I tillegg tilegnet han seg arbeidsgiverens hemmelige anbud på et prosjekt verd ca. 200 millioner kroner, ved å overføre datafilen med anbudet til sin private frisurf e-postkonto. For disse handlingene ble han tiltalt for grov økonomisk utroskap og grovt tyveri, jf. straffeloven §§ 275, jf. 276 og §§ 257, jf. 258. Mens han ble domfelt for grovt økonomisk utroskap ble han frifunnet for tyveriet, fordi data etter tingrettens oppfatning ikke kunne anses som «løsøregjenstand», jf. straffeloven § 257. Som støtte for tolkningen ble det vist til eldre oppfatninger i teorien, som er gjengitt i datakrimutredningen av 1985.

I forbindelse med lovtilpasningene 8. april 2005 som følge av tiltredelsen av datakrimkonvensjonen, påpekte flere høringsinstanser at vernet om data måtte styrkes slik at det kom på linje med det som gjelder for fysiske gjenstander. Fra ØKOKRIMs høringsuttalelse siteres (gjengitt fra Ot.prp.nr 40 (2004-2005) kapittel 3.2.5 side 14):

«ØKOKRIM har registrert en økning i henvendelser som gjelder «tyveri» av informasjon ved hjelp av en datamaskin, men hvor det vanskelig kan sies å foreligge brudd på en beskyttelse. Et typeeksempel er en utro tjener i en bedrift som uberettiget kopierer ut informasjon til en konkurrent.

I en tid hvor man tillegger IKT-tjenester stadig større verdi, bør det strafferettslige vern om data i hvert fall være på linje med det man har for gjenstander, og som kjent stilles det ikke noe vilkår om at en gjenstand skal være beskyttet for at det skal være tale om tyveri.»

Justisdepartementet fulgte opp med følgende bemerkning (Ot.prp. nr. 40 (2004-2005) kapittel 3.2.6 side 14-15):

«I lys av høringen er det etter departementets syn naturlig å se spørsmålet om å endre straffeloven § 145 annet ledd i sammenheng med reglene om uberettiget tilegnelse av informasjon, selv om disse regelsettene retter seg mot ulike stadier av et hendelsesforløp og heller ikke fullt ut varetar de samme hensyn. Ulike former for «informasjonstyveri» synes å utgjøre et økende samfunnsmessig problem, som det kan være grunn til å møte med nye lovtiltak. På bakgrunn av særlig ØKOKRIMs høringsuttalelse, som får støtte av Politidirektoratet, ser departementet et klart behov for å utrede nærmere om data i dag har et for svakt strafferettslig vern sammenlignet med for eksempel vernet mot tyveri av fysiske gjenstander. Å vurdere dette og eventuelt utforme en helt ny bestemmelse som rammer urettmessig tilegnelse av informasjon, slik ØKOKRIM foreslår, er imidlertid en oppgave av en slik art at det er naturlig å la den gå inn i Datakrimutvalgets videre arbeid. Det synes med andre ord som om reformbehovet innenfor dette feltet strekker seg utover en eventuell endring av straffeloven § 145 annet ledd slik som skissert i høringsbrevet.»

Justiskomiteen sa seg enig i at «dagens lovgivning ikke er fullgod på alle områder» (Innst. O. nr. 53. (2004-2005) kapittel 2).

I stedet for å avvente en ny utredning fra Datakrimutvalget valgte komiteen å fjerne beskyttelsesvilkåret i straffeloven § 145 annet ledd.

Datakrimutvalget foreslår at det strafferettslige vern om data og informasjon styrkes slik at det kommer på linje med vernet for løsøregjenstander. De to viktigste tiltakene er å sørge for straffebud som rammer uberettiget tilegnelse av data og databasert informasjon, og etterfølgende befatning med slikt straffbart utbytte. I dag oppnås et visst vern for data ved en fortolkning av gjenstandsbegrepet i de tradisjonelle straffebud. Etter gjeldende rett omfattes ikke data av begrepet «gjenstand» i straffeloven, og har følgelig ikke selvstendig beskyttelse etter de regler som anvender dette begrepet. Legaldefinisjonen av «løsøregjenstand» i straffeloven § 6 er ikke begrenset til fysiske gjenstander, men omfatter også «enhver til Frembringelse af Lys, Varme eller Bevægelse fremstillet eller opbevaret Kraft».

Dette omfatter elektrisitet og andre energiformer, men ikke data, jf. Matningsdal og Bratholm: Straffeloven Kommentarutgave, Bind I side 31. Ny straffelov § 12 har følgende definisjon av «gjenstand»: «Med gjenstand menes også elektrisk energi eller annen energi». Forarbeidene presiserer: «informasjon i datasystemer mv. skal fortsatt ikke regnes som gjenstand», jf. Ot.prp. nr. 90 (2003-2004) kapittel 12.2.4 side 165.

Data er derfor ikke vernet etter straffebud som benytter begrepet «gjenstand» i ny straffelov heller.

Etter gjeldende rett fortolkes imidlertid «gjenstand» utvidende i enkelte sammenhenger og kan da omfatte data som er lagret. Tolkningen, som kalles å anvende det «funksjonelle gjenstandsbegrep», ser dataene i sammenheng med det fysiske lagringsmediet som utvilsomt er en gjenstand. På denne måten har man i rettspraksis funnet å kunne anvende straffebudet om skadeverk på «gjenstand» i straffeloven § 291, i saker om uberettiget endring og sletting av data. Det kan blant annet vises til bakdør-kjennelsen i Rt. 2004 side 1619, hvor uberettigete endringer i programoppsettet ble ansett som straffbart etter straffeloven § 291.

Denne fortolkningsteknikken har sitt opphav i den såkalte «damlukedommen» i Rt. 1930 side 1005. Anvendt på data er fortolkningen noe av en konstruksjon og gir heller ikke tilstrekkelig vern stilt overfor det behov som foreligger. Det vises til drøftelsen i Sunde 2006 «Lov og rett i cyberspace» kapittel 4, med en kritikk av denne tolkningsmetoden i datatilfeller. Et viktig hensyn er at gjenstandsbegrepet må fortolkes i lys av de øvrige vilkår i det straffebud som det er tale om at skal gis anvendelse på data. For så vidt gjelder tyveribestemmelsen skaper vilkåret «borttar» problemer, siden «datatyveri» typisk skjer ved kopiering eller overføring av data. Disse handlingene fordrer ikke at de originale data forflyttes. Man kan si at vilkåret «borttar» ikke er oppfylt, eller at begrepet «gjenstand» slik det benyttes i straffeloven § 257 ikke omfatter data.

Videre reiser etterfølgende bruk av data og databasert informasjon som er uberettiget tilegnet noen særlige spørsmål som gjør at straffelovens

bestemmelser om heleri og sikringshandlinger i straffeloven § 317 første og annet ledd neppe er helt tilstrekkelige, se kapittel 5.5.3.

Også andre typer straffebud kan bidra til et styrket vern om data. Regler som verner om de datasystemer og elektroniske kommunikasjonsnett som lagrer, behandler og overfører data gir et indirekte vern. Både de tidligere nevnte straffebud som omfatter handlinger som skaper stor fare for annen datakriminalitet og straffebudene om datainnbrudd, datamodifikasjon og driftshindring m. fl. gir et styrket vern om data og databasert informasjon.

I det følgende gis det en nærmere beskrivelse av hensynene bak reglene om uberettiget tilegnelse og etterfølgende befatning med databasert informasjon og data, jf. utkastet §§ 5, 6 og 9. De konkrete formuleringene i straffebudene er kommentert i kapittel 9.5, 9.6 og 9.9.

### 5.5.2 Uberettiget tilegnelse av data og databasert informasjon

Utkastet §§ 5 og 6 gir et generelt strafferettslig vern mot tilegnelse av «data» og «databasert informasjon».

*Tilegnelse av data, jf. utkastet § 6*

«Data» er enhver representasjon av informasjon som lagres eller behandles av et datasystem, eller overføres i et elektronisk kommunikasjonsnett, jf. utkastet § 1 bokstav c. I tillegg omfattes enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk utstyr, jf. bestemmelsens annet punktum.

Tilegnelseshandlinger etter utkastet § 6 fordrer følgelig bruk av et datasystem eller annet teknisk utstyr, siden handlingen er rettet mot signaler som bare kan utnyttes maskinelt. Når tilegnelsen gjelder data som er lagret eller som behandles vil den bestå i en kopieringshandling. Kopiering innebærer at data overføres til et annet fysisk lagringsmedium eller nettsted enn der hvor de originale data befinner seg, og som er utenfor den berettigetes kontroll. For tilegnelse av data som er lagret, er fremgangsmåtene benyttet av domfelte i tingrettsdommen nevnt i kapittel 5.5.1 (TOSLO-2004-84792) illustrerende. Domfelte hadde kopiert data fra arbeidsgivers produksjonsserver til flere cd-rom og dessuten overført data som vedlegg til en e-post.

Tilegnelse av data som er under overføring kan kalles «tapping». Tapping betyr at kommunikasjonsstrømmen fortløpende kopieres til et lagringsmedium mens den er underveis til mottaker. Tappingen vil ikke nødvendigvis påvirke overføringen som sådan, slik at selve kommunikasjonen kan skje uforstyrret.

*Tilegnelse av databasert informasjon, jf. utkastet § 5*

Utkastet § 5 første ledd bokstav a retter seg mot tilegnelse av «databasert informasjon». «Databasert informasjon» er meningsinnholdet i data, jf. utkastet § 1 bokstav d. Databasert informasjon oppstår når man gjør seg kjent med innholdet i data, og fordrer sansebruk av et menneske. Tilegnelse av databasert informasjon som er lagret kan for eksempel skje ved å lese innholdet på et skjermbilde eller ved å lytte til et opptak av en samtale. Når opptaket er lagret er det å anse som «data», jf. utkastet § 1 bokstav c, mens det transformeres til «databasert informasjon» ved avspilling, jf. utkastet § 1 bokstav d. Tilegnelse av det lagrede opptaket kan skje maskinelt ved kopiering og rammes i så fall av utkastet § 6. Men tilegnelse kan også skje ved avspilling, det vil si at lovovertrederen lytter til og/eller ser på innholdet. I så fall kommer utkastet § 5 til anvendelse.

Tilsvarende gjelder i overføringstilfellene. Ved kopiering av signalstrømmen til et lagringsmedium skjer en tilegnelse av data (som overføres i et elektronisk kommunikasjonsnett, jf. utkastet § 1 bokstav c), jf. utkastet § 6. Hvis noen lytter eller ser på overføringen mens den foregår (i sann tid) foreligger tilegnelse av databasert informasjon, jf. utkastet § 5, fordi det skjer sansebruk av et menneske. Dersom kommunikasjonen kopieres til et lagringsmedium samtidig som man foretar avlytting, foreligger overtredelse både av utkastet §§ 5 og 6.

*Papirutskrift*

Det anses nødvendig å bygge ut utkastet § 5 for å fange opp den praktiske form for informasjonstilegnelse som skjer ved utskrift av data. Tatt i vid forstand kan uttrykket «databasert informasjon» forstås å omfatte tegn i ethvert trykt skrift som er fremstilt ved hjelp av datastyrte trykke- og kopieringsprosesser. Så vidt skal imidlertid ikke uttrykket forstås, noe som klart følger av definisjonens tilknytning til datadefinisjonen, se utkastet § 1 bokstav d, jf. bokstav c og merknadene i kapittel 9.1 og 9.5. Dette innebærer at en utskrift fra en datamaskin *ikke* er meningsinnhold i «data». Hovedregelen er at trykte skrifter anses om løsøregjenstand og gis vern mot uberettiget tilegnelse etter reglene om tyveri og underslag (det tenkes ikke her på det opphavsrettslige vernet).

Det antas imidlertid å være behov for en utvidelse av området for utkastet § 5 i tilfeller som gjelder uberettiget tilegnelse av utskrift fra en datamaskin, på grunn av den nære sammenhengen handlingen har med et informasjonstyveri direkte fra skjermen eller spilleren.

Det er nærliggende å tenke seg at uberettiget tilegnelse av informasjon kan skje ved at lovovertrederen ser sitt snitt til å ta en utskrift, for eksempel av et skjermbilde når han er på besøk hos en konkurrent. Det kan tenkes at borttagelse av en utskrift kan straffes etter reglene om tyveri og naskeri, jf. straffeloven §§ 257 og 391a. Men rettsanvendelsen treffer noe på siden av det straffverdige ved handlingen, som er selve *informasjonstilegnelsen*, og denne kan innebære en langt større krenkelse overfor den som blir rammet enn det som i hvert fall ville følge av naskeribestemmelsen. Siden det å bortta en slik utskrift står i meget nær sammenheng med de andre tilegnelsestilfellene som omfattes av utkastet § 5, er det naturlig å bygge ut bestemmelsen til å omfatte dette. Det er gjort ved alternativet i utkastet § 5 første ledd bokstav b, som omfatter *«utskrift av databasert informasjon»*. Det kreves ikke at lovovertrederen selv har tatt utskriften, bare at utskriften står i så nær sammenheng med datasystemet at utskriften i det konkrete tilfellet nærmest kan anses som en forlengelse av datasystemet. Den kan for eksempel ligge klar til avhenting i en kassett i utskriftsmaskinen (printeren), og så ser lovovertrederen sitt snitt til å ta den med seg når han går forbi.

De grensespørsmål som kan oppstå overfor tyveribestemmelsen må nødvendigvis løses i rettspraksis. Bestemmelsens annet ledd inneholder en subsidiaritetsklausul som gir tyveribestemmelsen forrang der det er naturlig. Dette er en lovteknikk som i dag blant annet er benyttet i straffeloven § 275 tredje ledd, som regulerer forholdet mellom underslag og økonomisk utroskap.

### *Harmoniserings- og konkurrensspørsmål*

Selv om data og databasert informasjon ikke har et selvstendig strafferettslig vern etter gjeldende rett, rammer flere straffebud handlinger som reelt sett innebærer en slik tilegnelse. Dette gjelder straffeloven §§ 145 annet ledd og 262 annet ledd, samt åndsverkloven § 53a første ledd, jf. § 54 første ledd bokstav b. Direkte rammer de nevnte bestemmelser den uberettigete tilgang, jf. «skaffer seg adgang», «bruk av dekodingsinnretning» og «omgå effektive tekniske beskyttelsessystemer». Den umiddelbare følge av de nevnte handlinger er imidlertid *tilegnelse,* enten av data eller databasert informasjon. Tilegnelsen skjer ved at dataene eller den databaserte informasjon leses maskinelt og eventuelt kopieres, at fjernsynssignaler dekodes til klart innhold som fremvises på fjernsynsskjerm, at en dvd-film kopieres i ubeskyttet tilstand (datatyveri) og avspilles (informasjonstyveri) eller at krypterte informasjonssamfunnstjenester tappes under overføring (datatyveri) og deretter avspilles på gjerningspersonens eget utstyr (informasjonstyveri).

Som det har fremgått rammes disse handlingene av utkastet §§ 5 og 6. Selve den uberettigete tilgang til lagrede data – som er den forutgående handling – rammes av utkastet § 4 (ulovlig tilgang til datasystem). Det vises til kapittel 5.6.2 i underkapitlene «Særlig om ulovlig tilgang til frittstående lagringsmedier» og «Harmoniseringsspørsmål». I mange tilfeller vil det være naturlig å anvende utkastet § 4 i realkonkurrens med utkastet §§ 5 eller 6. Dermed får man bedre frem enn etter dagens regler at slike krenkelser består både av uberettiget tilgang og en straffbar tilegnelse.

Uberettiget dekoding og tilegnelse av data og databasert informasjon under overføring rammes i sin helhet av utkastet §§ 5 og 6. Det vil her gjerne være sammenfall mellom dekodingen og tilegnelsen, noe som illustreres ved piratdekoding av fjernsynssignaler nevnt ovenfor. Som følge av dekodingen fremvises programmet på fjernsynsskjermen. Hvorvidt det er naturlig å anvende utkastet §§ 5 og 6 i konkurrens der det først skjer en datakopiering og deretter en avspilling, kan være tvilsomt. I slike tilfelle kan det kanskje være mer naturlig å se informasjonstilegnelsen som en konsekvens av datatyveriet og eventuelt som en straffskjerpende omstendighet ved dette. Dette konkurrensspørsmålet antas å finne sin naturlige løsning i rettspraksis.

En annen sak er at utkastet §§ 5 og 6 kan anvendes i konkurrens med utkastet § 9 som gjelder etterfølgende befatning med slikt straffbart utbytte. Overtredelse av utkastet § 9 er en ny selvstendig straffbar handling og det spiller ingen rolle for straffbarheten om lovovertrederen også begikk primærovertredelsen, det vil si, overtredelsen av utkastet §§ 5 eller 6. Utkastet § 9 kan anvendes både der lovovertrederen har begått primærlovbruddet og når befatningen skjer av en tredjeperson.

Til slutt kan det nevnes at utkastet § 8 om uberettiget bruk av datasystem m.v. ofte vil være aktuell i konkurrens med utkastet §§ 5 og 6. «Bruk» etter utkastet § 8 må imidlertid gjelde den side av handlingen som ikke kan karakteriseres som *tilegnelse*, for eksempel den bruk som går ut på å lete i datasystemet etter data som skal tilegnes.

### 5.5.3 Etterfølgende befatning med data og databasert informasjon som er utbytte av en straffbar handling

En styrking av det generelle vern for data og databasert informasjon reiser spørsmål om det er behov for et eget straffebud om etterfølgende befatning når data og databasert informasjon er utbytte av en straffbar handling. Det kan være tale om en tredjeperson som mottar slikt utbytte eller om tyvens (primærforbryterens) etterfølgende disposisjoner over utbyttet. Som et eksempel kan man tenke seg at tyven legger en mengde kredittkortnumre han uberettiget har kopiert fra en database, ut på internett. Ved å eksponere data som skulle vært konfidensielle kan han ramme omdømmet til innehaveren av databasen og kortinnehaverne og påføre kortutstederne økonomisk tap.

Det er naturlig å ta utgangspunkt i straffeloven § 317 slik bestemmelsen lyder etter lovendringen 30. juni 2006 nr. 49, som trådte i kraft straks. Første ledd er delt i to alternativ som rammer heleri og hvitvasking av utbytte av en straffbar handling. Helerialternativet rammer den som «mottar eller skaffer seg eller andre del i utbytte av en straffbar handling».

Alternativet rammer en tredjeperson som mottar eller har annen direkte befatning med utbyttet for seg selv eller for en annen.

Hvitvaskingsalternativet rammer den som «yter bistand til å sikre slikt utbytte for en annen».

Det kan for eksempel være tale om en advokat eller annen profesjonell rådgiver som bistår med å konvertere utbyttet slik at forbindelsen til den opprinnelige straffbare handling skjules. Også bistand som ytes til heleren for å skjule utbyttet rammes av dette alternativet (Matningsdal og Bratholm: Straffeloven Kommentarutgave, Bind II side 851). Verken heleri- eller hvitvaskingsalternativet kommer til anvendelse overfor den som har initiert eller bistått ved utførelsen av primærforbrytelsen. I stedet blir han å straffe for medvirkning til denne.

Før lovendringen i 2006 var det klart at en tyv eller en bedrager ikke ble straffet for sin ytterligere befatning med tyvegodset. Dette fremgår av Rt. 2003 side 1376 hvor Høyesterett uttalte i avsnitt 29:

> «Spørsmålet blir etter dette om man markerer ytterligere sider ved den straffbare handling om hun i tillegg straffes for heleri. I denne sammenheng nevner jeg at i forhold til det tilsvarende spørsmål ved tyveri, straffes ikke tyven i tillegg for underslag eller heleri for sin videre befatning med tyvegodset, jf. Bratholm/Matningsdal: Straffeloven med kommentarer, Bind II side 663 med videre henvisninger. Dette standpunktet begrunnes i at tyvens senere disposisjon over tyvegodset i forhold til fornærmede konsumeres av den tilegnelsen som har skjedd ved tyveriet. Selv om verken merverdiavgiftsloven §72 nr. 1 eller straffeloven §270 har som straffbarhetsvilkår at det skjer en tilegnelse, må den begrensningen som er oppstilt ved tyveri, gjelde tilsvarende.»

Det vises også til Ot.prp. nr. 53 (2005-2006) side 20. Her uttalte departementet:

> «Etter gjeldende norsk rett anses det ikke straffbart for en lovbryter å foreta handlinger for å sikre utbyttet for seg selv. Heleribestemmelsen kan for eksempel ikke anvendes i konkurrens med straffebudet mot tyveri eller bedrageri, se bl.a. Rt-2003-1376 med videre henvisninger. Standpunktet er begrunnet med at lovovertrederens senere disposisjon over for eksempel tyvegodset konsumeres av tilegnelsen som er skjedd ved tyveriet, og det samme er lagt til grunn ved bedrageri selv om det der ikke er noe vilkår om tilegnelse.»

For heleri var forholdet mer usikkert. Det vises til Matningsdal og Bratholm: Straffeloven Kommentarutgave, Bind II side 856-860.

Ved lovendringen i 2006 ble det tilføyd et nytt annet ledd som skal ramme såkalte «sikringshandlinger», det vil si primærforbryterens egen befatning med utbyttet. Bestemmelsen i straffeloven § 317 annet ledd lyder:

> «For hvitvasking straffes også den som gjennom konvertering eller overføring av formuesgoder eller på annen måte skjuler eller tilslører hvor utbyttet fra en straffbar handling han selv har begått, befinner seg, stammer fra, hvem som har rådigheten over det, dets bevegelser, eller rettigheter som er knyttet til det.»

Lovendringen skjedde for å gjennomføre FN-konvensjonen mot korrupsjon av 31. oktober 2003 artikkel 23, som er rettet mot hvitvasking av utbytte av en straffbar handling. Det vises til den nærmere behandling i St.prp. nr. 49 (2005-2006) side 23-25.

Det antas at straffeloven § 317 annet ledd også rammer en eventuell medvirker til primærforbrytelsen. Straff etter § 317 annet ledd kan altså anvendes i konkurrens med straff for primærforbrytelsen, og av motivene fremgår det at annet ledd *skal* brukes i konkurrens med straffebudet som rammer primærforbrytelsen «dersom først vilkårene i annet ledd er oppfylt», jf. Ot.prp. nr. 53 (2005-2006) side 36.

Etter gjeldende rett anses det å være klart at data og informasjon som er tilegnet ved en straffbar handling omfattes av utbyttebegrepet i straffe-

loven § 317. Dette begrepet omfatter som kjent langt mer enn fysiske gjenstander, for eksempel fordringer som ikke er knyttet til noe gjeldsbrev og immaterielle rettigheter. Det kan også vises til pinkodekjennelsen (Rt. 1995 side 1872) hvor det ble lagt til grunn at en stjålet pinkode til et telefonkort var omfattet. Høyesterett uttalte at

> «PIN-kodene gir tilgang til telefonselskapenes tjenester, og de har derved økonomisk betydning og er egnet til å bli disponert over. En PIN-kode må derfor anses som et utbytte i straffeloven §317 første ledds forstand når den skriver seg fra en straffbar handling.»

Denne lovforståelsen er også lagt til grunn i Romerike tingretts dom av 25. november 2003 (passorddommen), hvor det ble avsagt dom på heleri av minst 650 000 brukernavn og passord som tilhørte brukerne til en internettleverandør.

Vilkåret om at utbyttet må stamme fra en straffbar handling har i stor grad utelukket muligheten for å anvende straffeloven § 317 på data og informasjon. Siden det ikke har foreligget noe straffebud som generelt har rammet uberettiget data- og informasjonstilegnelse, har det vært problematisk å påvise en primærforbrytelse. Dersom nye straffebud om uberettiget data- og informasjonstilegnelse blir gjennomført slik utvalget foreslår, vil også det etterfølgende vernet bli styrket. Straffeloven § 317 vil bli mer anvendelig på data og informasjon som følge av at utkastet §§ 5 og 6 kriminaliserer den uberettigete tilegnelsen.

Straffeloven § 317 annet ledd rammer den som skjuler eller tilslører hvor utbyttet fra en straffbar handling han selv har begått befinner seg, stammer fra, hvem som har rådigheten over det, dets bevegelser eller rettigheter som er knyttet til det. Det er dette som karakteriserer hvitvasking. For øvrig er det regnet opp måter dette kan gjøres på, nemlig ved konvertering, overføring av formuesgoder eller på annen måte.

Det presiseres at den folkerettslige forpliktelsen til å kriminalisere er begrenset til å gjelde sikringshandlinger. Lovgiver valgte ikke å gå lenger enn det som var nødvendig for en lojal gjennomføring av den folkerettslige forpliktelsen. Forarbeidene presiserer også at den rene besittelse av utbyttet fra en straffbar handling man selv har begått ikke rammes (Ot.prp. nr. 53 (2005-2006) side 36).

Det fremgår videre av Ot.prp. nr. 53 (2005-2006) side 21-22 at det ikke er meningen med lovendringen å dekke befatning med utbyttet som allerede er dekket gjennom gjerningsbeskrivelsen i primærlovbruddet, med den nye hvitvaskingsbestemmelsen. Det heter i Innst.O. nr. 60 (2005-2006) i kapittel 1.4.1.1:

> «Departementet tolker artikkel 23 nr. 1 slik at det ikke er påkrevd å kriminalisere særskilt ervervet, besittelsen eller bruken av formuesgoder når det er den som har begått primærlovbruddet som har slik befatning med utbyttet. Det som kreves kriminalisert er sikringshandlinger som f. eks. konvertering eller overføring av utbyttet fra en annen straffbar handling som man selv har begått. »

Dette innebærer at straffeloven § 317 annet ledd rammer tyvens eller helerens etterfølgende realisasjon av tyvegods hvis det skjer som ledd i hvitvasking av utbytte. En ordinær realisasjon av tyvegods som ikke har dette som formål, vil etter utvalgets vurdering ikke rammes av bestemmelsen.

Bestemmelsens rekkevidde drøftes nærmere i tilknytning til tre typetilfelle som påkaller en viss interesse. Tilfellene gjelder primærforbryterens (og medvirkerens) disposisjoner over utbyttet. Problemstillingen er om straff kan anvendes for etterfølgende disposisjoner i konkurrens med straff for primæroverтredelsen.

Tilfellene er som følger:

- Primærforbryteren selger eller overfører på annen måte utbyttet til en tredjeperson. Det er klart at mottakeren kan straffes for heleri, jf. § 317 første ledd. Spørsmålet er om primærforbryteren kan rammes for overføringen av det utbyttet han selv ulovlig har tilegnet seg, jf. utkastet §§ 5 og 6.
- Primærforbryteren legger data han rettsstridig har tilegnet seg ut på internett. Motivet kan variere. Det kan for eksempel skyldes et behov for å demonstrere ferdigheter, hvor dataene tjener som bevis for at han har lykkes i å trenge seg inn i et datasystem og stjele informasjon. Et annet eksempel kan være at handlingen skyldes et ønske om å skade omdømmet til innehaveren av datasystemet hvorfra dataene er stjålet. Tankegangen er da at omdømmet skades dersom data som skulle vært behandlet konfidensielt er blitt gjort allment tilgjengelige. Det vises for så vidt til eksemplet nevnt innledningsvis.
- Primærforbryteren utnytter de stjålne data eller informasjon i egen virksomhet. Han driver for eksempel en konkurrerende virksomhet i forhold til den rette innehaveren av dataene. Som eksempel kan man tenke seg at innehaveren av en bedrift ved overtredelse av utkastet §§ 4-6, skaffer seg adgang til kunderegisteret til kon-

kurrenten, som han kopierer og bruker som grunnlag for å sende ut konkurrerende markedsføringshenvendelser. Et tilfelle fra foreleggspraksis er omtalt i Sunde 2006 «Lov og rett i cyberspace» side 164-165. Her hadde en person kopiert kunderegisteret og solgt det til en konkurrerende bedrift som utnyttet det i sin virksomhet. Det ble gitt forelegg for overtredelse av straffeloven § 145 annet ledd (for vedkommende som hadde trengt seg inn og kopiert dataene) og straffeloven § 317 (mottakeren av dataene). Den foreliggende problemstilling gjelder om datainntrengeren, dersom vedkommende hadde anvendt kunderegisteret selv, også bør kunne straffes for dette.

Utvalget antar at de nevnte tilfeller er klart straffverdige forhold som det er behov for å ramme. I hvert fall er det viktig å påse at det rettslige vernet om data og databasert informasjon er på linje med det rettslige vernet om annen type utbytte av straffbare forhold.

På et vesentlig punkt avviker imidlertid data og databasert informasjon fra andre former for utbytte. Selv om data eller databasert informasjon er stjålet, er eieren som regel ikke fratatt besittelsen av originaldataene. Eierens filer er fortsatt komplette, men de er kopiert av tyven. Den økonomiske verdien av data og databasert informasjon er gjerne betinget av at den er konfidensiell. Etter en ulovlig tilegnelse er konfidensialiteten brutt. Bedriftshemmeligheter kan ha blitt kjent. Dette kan for eksempel gjelde teknologi, strategiplaner og finansielle forhold. De hemmelige valgkampplanene til et politisk parti kan ha kommet på avveie. Det samme kan gjelde opplysninger om personlige forhold, for eksempel helseopplysninger. Full restitusjon av dataene eller den databaserte informasjonen til rette innehaver kan fremstå som umulig og meningsløst. Vedkommende kan eventuelt kompenseres gjennom erstatning, noe som kan fremstå som et lite tilfredsstillende alternativ, blant annet på grunn av problemer med å kalkulere skadeomfang og årsakssammenheng.

Dette rører ved den del av begrunnelsen bak de strenge hvitvaskingsreglene som gjelder at slike handlinger medfører «at det blir vanskeligere å finne frem til formuesgodene igjen og returnere dem til eieren, selv om primærlovbruddet blir oppklart» (Ot.prp. nr. 53 (2005-2006) side 21 i kapittel 4.7.2.2). Momentet står enda sterkere ved utnyttelse av data og databasert informasjon hvor restitusjon for alle praktiske formål vil være utelukket, selv om det er på det rene hvor informasjonen er og hvordan den er blitt utnyttet.

Felles for de tre typetilfellene er at gjerningspersonens etterfølgende handling har karakter av å være en endelig disposisjon over utbyttet. Spørsmålet er om dette rammes av straffeloven § 317 annet ledd, hvoretter formålet er å ramme handlinger som «skjuler eller tilslører» utbyttets forbindelse med den opprinnelige straffbare handling.

Ordlyden angir som nevnt ovenfor hvilke etterfølgende disposisjoner som rammes, nemlig «konvertering eller overføring av formuesgoder eller på annen måte». Med alternativet «på annen måte» er ordlyden så vid at i realiteten enhver disposisjon utover det rene forbruk er omfattet. Begrensningen av bestemmelsen ligger i neste del av regelen, som forutsetter at de nevnte handlinger innebærer at gjerningspersonen «skjuler eller tilslører hvor utbyttet [...] befinner seg, stammer fra, hvem som har rådigheten over det, dets bevegelser, eller rettigheter som er knyttet til det».

De tre nevnte eksempler gjelder realisasjon av utbyttet (salg/overføring), det å gjøre utbyttet tilgjengelig for andre eller utnytte utbyttet direkte i egen virksomhet. Handlingene innebærer en direkte og endelig utnyttelse av utbyttet. Spørsmålet er om de kan anses som sikringshandlinger, jf. straffeloven § 317 annet ledd. Så vidt forstås tar denne bestemmelsen i utgangspunktet sikte på handlinger som sikrer utbyttet for gjerningspersonen, og ikke på den endelige utnyttelse av utbyttet.

I forhold til de nevnte typetilfelle er det neppe helt klart hva som er rekkevidden av straffeloven § 317 annet ledd. Dette kan bero på de konkrete omstendigheter i den enkelte sak.

Første eksempel som gjelder salg eller overføring, er en form for «konvertering», jf. annet ledd. Vederlaget sikrer utbyttet for gjerningspersonen i form av et surrogat. Dette omfattes, jf. første ledd siste punktum. Konvertering til et økonomisk vederlag kan sies å tilsløre hvor utbyttet «stammer fra», jf. annet ledd, men det kan reises tvil om konvertering som kun tar sikte på å realisere en økonomisk gevinst omfattes av bestemmelsen.

Det antas derfor at det første typetilfellet – tyvens salg av stjålne data eller informasjon – i enkelte tilfeller kan rammes av straffeloven § 317 annet ledd, men at det er svært tvilsomt hvor langt bestemmelsen rekker.

Annet eksempel gjelder at stjålet informasjon gjøres tilgjengelig på internett. For så vidt gjelder tilgangskoder inneholder lovforslaget en spesialbestemmelse som vil ramme slik tilgjengeliggjøring, enten tilgangskoden er utbytte av en straffbar handling eller ikke (den er for eksempel gjettet), jf. utkastet § 10. Se også gjeldende bestemmelse i straffeloven § 145b. Utenfor området til utkastet

§ 10, antas imidlertid slik tilgjengeliggjøring i sin generelle form å falle utenfor straffeloven § 317 annet ledd. Det man får igjen for tilgjengeliggjøringen i form av en eventuell forbedret status i visse miljøer eller glede over den skade som måtte være forvoldt, faller utenfor utbyttebegrepet. Det kan derfor ikke være tale om å bedømme tilgjengeliggjøringen som noen konverterings- eller sikringshandling.

Det tredje og siste typetilfellet gjelder primærforbryterens egen bruk av den ulovlig tilegnede databaserte informasjon eller data. Som nevnt skal straffeloven § 317 annet ledd avgrenses mot den rene besittelse. Bruk er imidlertid en aktiv handling som innebærer at gjerningspersonen kan nyttiggjøre seg utbyttet. Vedkommende tar for eksempel konkurrentens teknologi i bruk i egen produksjon. For så vidt gjelder data og databasert informasjon antas det at den etterfølgende utnyttelse ofte kan ha meget stor verdi for gjerningspersonen, for eksempel i tilfeller av industrispionasje. Hvis gjerningspersonen gjør endringer i informasjonen for å skjule opprinnelsen, kommer straffeloven § 317 annet ledd til anvendelse, jf. «på annen måte tilslører hvor utbyttet stammer fra». Har han stjålet et dataprogram kan han foreta endringer i kildekoden for å skjule opprinnelsen før han selv tar programmet i bruk. Dette vil representere en sikringshandling som rammes av straffeloven § 317 annet ledd, og som kommer i tillegg til selve utnyttelsen av programmet. Ordlyden ses imidlertid ikke å ramme den endelige utnyttelsen.

Til slutt må det tilføyes at det kan oppstå spørsmål om foretaksstraff for heleri av dataene eller den databaserte informasjonen, for foretaket som mottar utbyttet og utnytter det i virksomheten. Informasjonstyvens forhold er straffbart etter utkastet §§ 5 og 6, og kan etter omstendighetene være straffbart som en konverteringshandling etter straffeloven § 317 annet ledd, dersom informasjonen er solgt til bedriften, jf. bemerkningene ovenfor. Bedriftens *mottak* er et heleri som er straffbart etter første ledd. Videre er det spørsmål om bedriften (heleren) kan straffes for den etterfølgende utnyttelse av dataene eller informasjonen i virksomheten. Det antas at dette må løses på samme måte som for den første gjerningsperson (tyven), med andre ord at heleriet kan anses som en primærforbrytelse i relasjon til annet ledd. Helerens handlinger kan altså etter omstendighetene straffes både etter § 317 første og annet ledd.

Imidlertid er det uansett et spørsmål om utnyttelsen av dataene og den databaserte informasjonen som sådan, kan rammes av annet ledd, og det er denne uklarheten som begrunner behovet for et eget straffebud, jf. utkastet § 9. Problemene ved anvendelsen av straffeloven § 317 annet ledd tilsier at det er behov for en egen bestemmelse som klart rammer både primærforbryterens og helerens etterfølgende befatning med ulovlig tilegnet informasjon og data. Det foreslås at også handlinger som nok kan omfattes av uttrykket «konvertering» bør omfattes av spesialregelen, siden det som nevnt kan være tvilsomt hvor langt § 317 annet ledd rekker i slike tilfeller. Formålet må være ikke bare å ramme sikringshandlinger, men også handlinger som bærer preg av å være den endelige disponering, utnyttelse eller forbruk av ulovlig tilegnet data eller informasjon. Dette anses å være viktig siden data og informasjon sjelden kan restitueres til rette eier. Det vises også til bemerkningene om de problemer som gjør seg gjeldende i forhold til mulighetene for erstatning, for eksempel i tilfeller der de stjålne data er spredt på internett i skadehensikt.

Meningen er at utkastet § 9 skal være en spesialregel for etterfølgende befatning med data og databasert informasjon som er utbytte av en straffbar handling. Utvalget har vurdert om den straffbare handling bør kvalifiseres i lovteksten, for eksempel ved at det må være tale om en overtredelse av utkastet §§ 5 eller 6. Utvalget har kommet til at dette ikke er ønskelig, siden det er behov for å styrke lovverket mot data- og informasjonsheleri m.v. uavhengig av karakteren av primærovertredelsen. Man kan for eksempel tenke seg etterfølgende befatning med data som er skaffet til veie ved elektronisk kartlegging av datasystem, jf. utkastet § 2. Heller ikke straffeloven § 317 anvender noe kvalifikasjonskrav til primærovertredelsen. Det er tilstrekkelig at det er tale om en «straffbar handling». Utvalget har etter dette kommet til at primærovertredelsen bør angis generelt, dog slik at det er tale om en handling som er straffbar etter reglene i datakrimkapitlet.

Dersom vilkårene for straff er oppfylt både etter straffeloven § 317 og utkastet § 9, skal utkastet § 9 anvendes, jf. *lex specialis prinsippet*. Det skal stilles de samme krav til praktisering av vilkårene i utkastet § 9 som etter straffeloven § 317. Det betyr at det ikke er noe vilkår for straff at det foreligger domfellelse for primærovertredelsen og det skal stilles tilsvarende krav til bevisstyrke m.v. som praktiseres etter straffeloven § 317. Også en primærovertredelse begått i utlandet er relevant i forhold til utkastet § 9. Det samme vil være tilfelle dersom den forutgående handling ikke kan straffes, for eksempel fordi gjerningspersonen ikke var strafferettslig tilregnelig.

## 5.6 Handlinger som rammer datasystemenes funksjonalitet, kapasitet og sikkerhet

### 5.6.1 Innledning

I kapittel 4.6 «Hensynet til datasystemers pålitelighet» er det redegjort for hvordan hensynene til konfidensialitet, integritet og tilgjengelighet, samt mekanismer for autentisering, danner betingelser som er nødvendige for å anse datasystemer som pålitelige. I det følgende redegjøres det for de straffebud som direkte ivaretar disse hensynene. Dette er utkastet § 4 (ulovlig tilgang til datasystem), § 7 (datamodifikasjon), § 8 (uberettiget bruk av datasystem m.v.), § 13 (driftshindring), § 14 (masseutsendelse av elektroniske meldinger) og § 15 (identitetstyveri og bruk av uriktig identitet).

### 5.6.2 Ulovlig tilgang til datasystem

*Intet vilkår om beskyttelsesbrudd*

Det foreslås et straffebud som rammer den som skaffer seg ulovlig tilgang til et datasystem, jf. utkastet § 4. Straffebudet inneholder ikke noe vilkår om at datasystemet må være beskyttet. Dette har flere årsaker. For det første innebærer et slikt vilkår at det strafferettslige vern forbeholdes den som allerede er sikret. For utvalget er det et viktig hensyn at straffebudene rammer straffverdige handlinger uavhengig av om fornærmede har hatt kyndighet til å sørge for sikkerhetstiltak eller ikke, se kapittel 4.5.1.

En tenkelig innvending er likevel at uten et beskyttelsesvilkår er det fare for at terskelen for det straffbare blir for lav slik at bestemmelsen kan ramme handlinger som ikke er straffverdige. Men som det vil fremgå gir ikke et beskyttelsesvilkår nødvendigvis en klar og hensiktsmessig avgrensning.

I praksis skjer uberettiget tilgang ved bruk av to alternative metoder, enten ved misbruk av passord eller ved bruk av verktøy til å skaffe seg ulovlig tilgang (exploits) til å misbruke en sårbarhet. Man kan tale om «passordinnbrudd» og «sårbarhetsinnbrudd» (se kapittel 3.4.1). I begge tilfeller vil rettsstriden normalt være på det rene for gjerningspersonen og et vilkår om beskyttelsesbrudd i tillegg har ikke noen reell betydning. Selve anstrengelsen det innebærer å forsere en hindring kan lede til at overtredelsen anses som grov, jf. utkastet § 18, som nevner «om lovbruddet er begått ved å bryte en beskyttelse» blant de momenter som særlig skal vektlegges. Momentet kan også få betydning ved straffutmålingen.

Også rettstekniske hensyn taler for at man unngår et vilkår om at datasystemet må være beskyttet. Et slikt vilkår kan gi opphav til flere uklarheter slik at regelen blir vanskelig å praktisere.

For det første kan det diskuteres om et datasystem virkelig er beskyttet bare fordi det er passordkontrollert, når det på samme tid er sårbart for inntrengning ved sårbarhetsinnbrudd.

For det annet kan det fortone seg kunstig å skille mellom beskyttede og ubeskyttede systemer i absolutt forstand. Vanligvis blir datasystemer sikkerhetsmessig oppdatert og skal derfor være beskyttet mot sårbarhetsinnbrudd. Men siden sårbarheter oppdages av personer som skaffer seg ulovlig tilgang raskere enn man klarer å oppdatere, vil systemene uansett være utsatt. Og selv om et datasystem ikke er tilgangskontrollert betyr det ikke at hele systemet står åpent. Innehaveren vil skjerme administratorfunksjonene mot tilgang fra omverdenen for å sikre seg kontroll med sikkerhet og funksjonalitet. Dermed er det bare det vanlige brukernivået som er åpent tilgjengelig på såkalte usikrede servere. Men for personer med ulovlig tilgang er det nettopp systemadministratornivået som er attraktivt fordi det gir styring med datasystemet, og et inntrengningsforsøk vil følgelig bli rettet mot dette. Inntrengning kan således skje med utgangspunkt i det brukerområdet man har lovlig tilgang til, eller direkte ved sårbarhetsinnbrudd uten å gå via brukerområdet.

For det tredje har ikke anvendelse av tilgangskontroll noen faktisk betydning for datainntrengning som skjer ved sårbarhetsinnbrudd. Utvelgelse av datasystemer som utsettes for datainnbrudd skjer gjerne ved elektronisk kartleggingsvirksomhet som avdekker sårbarheter som kan misbrukes, se kapittel 5.4.2. Siden tilgangskontrollen ikke har noen funksjon overfor denne inntrengningsmetoden, savner det ofte mening å anvende et vilkår om at datasystemet skal være beskyttet.

Av de nevnte grunner foreslås ikke noe vilkår om at datasystemet skal være beskyttet. Dette er i samsvar med den gjeldende utforming av straffeloven § 145 annet ledd, etter lovendringen av 8. april 2005 nr 16. Beskyttelsesvilkåret ble da slettet for å styrke vernet om data, se kapittel 5.5.1.

*Rettsstridsvilkåret*

Etter utvalgets syn gir rettsstridsvilkåret alene en tilstrekkelig avgrensning av straffebudets rekkevidde. Dette er vilkåret om at tilgangen må være «uberettiget».

Rettstridsvilkåret gjelder både objektivt og subjektivt, hvilket betyr at lovovertrederen må mangle

rettsgrunnlag for å skaffe seg tilgangen og han må være klar over at han er uten slik rett.

Det er den materielle rett til å skaffe seg tilgang til datasystemet som er avgjørende og denne rett avgjøres av andre regler enn de strafferettslige, for eksempel avtaler, retningslinjer, instruks, arbeidsrettslige regler, regler i kjøps- og avtaleforhold, opphavsrettslige regler m.v. Tekniske tilgangsrettigheter er ikke i seg selv tilstrekkelig til å anse tilgangen som berettiget. Dette har betydning i de tilfeller hvor tilgang skaffes ved bruk av tilgangsrettigheter som er knyttet til en status som er opphørt. Det kan for eksempel være tale om tilgangsrettigheter man hadde som ansatt i en bedrift eller som student ved universitetet. Treghet i slettings- og oppdateringsrutiner kan medføre at de gamle brukerrettighetene fungerer selv om ansettelses- eller studentforholdet er avsluttet. Siden det underliggende rettsforhold er avgjørende vil bruk av gamle tilgangsrettigheter i utgangspunktet være uberettiget. I situasjoner hvor det er tvilsomt hva den underliggende rett går ut på kan eksistensen av den gamle tilgangsrettigheten være et moment som inngår i en helhetsvurdering, og som kan tale for at tilgangen i det konkrete tilfellet likevel ikke kan sies å være uberettiget. I hvert fall kan det ha betydning for om kravet til forsett er oppfylt, fordi brukeren feilaktig kan ha trodd at han var berettiget til å skaffe seg tilgang siden han fremdeles hadde muligheten rent teknisk.

Et praktisk eksempel på et tilstrekkelig rettsgrunnlag er samtykke fra innehaveren av datasystemet. På internett er det vanlig å basere seg på slike samtykker ved tilgang til datatjenester som er allment tilgjengelige. Et annet spørsmål er hvor langt samtykket rekker når det gjelder hvilken bruk som kan gjøres av tjenesten. Den strafferettslige siden av dette spørsmålet er behandlet i tilknytning til utkastet § 8 om uberettiget bruk av datasystem, se kapittel 5.6.5.

Nedenfor er det vist hvordan utkastet § 4 blant annet kommer til anvendelse på uberettiget tilgang til datalagringsmedier med opphavsrettslig vernet materiale. Dette er tilfeller som etter gjeldende rett rammes av åndsverkloven § 53a første ledd. I forhold til slike handlinger inneholder åndsverkloven § 53a tredje ledd annet punkt, en rettsstridsreservasjon som gjelder «privat brukers tilegnelse av lovlig anskaffet verk på det som i alminnelighet oppfattes som relevant avspillingsutstyr». Lovforslaget gjør ingen endring i denne rettsstridsreservasjonen som vil være et gyldig grunnlag for å skaffe seg «tilgang» etter utkastet § 4. Se også de generelle kommentarene til rettsstridsreservasjonen i kapittel 5.3.4.

### *Vilkåret «hele eller del av et datasystem»*

Ved utformingen av straffebudet har det vært ønskelig å få frem en presisering av at den uberettigete tilgang er straffbar både om den rammer hele eller en del av datasystemet. Dette bidrar til å klargjøre straffbarheten av to praktiske tilfeller hvor rettstilstanden ellers kanskje kunne by på tvil.

Utgangspunktet er at bestemmelsen rammer uberettiget tilgang som skaffes av personer som savner enhver rett til datasystemet, såkalte eksterne gjerningspersoner. Dette er klart straffbart. Men av formuleringen «del av» rammes også tilgang av personer som har rett til å benytte datasystemet og som overskrider grensene for denne rett (såkalt *eskalering av brukerrettigheter*). Videre rammes tilfelle hvor lovovertrederen skaffer seg tilgang til innholdet på frittstående lagringsmedier som ikke alene oppfyller vilkåret for å være et «datasystem», se kommentarene til legaldefinisjonen i utkastet § 1 bokstav a, i kapittel 9.1. Slike lagringsmedier kan for eksempel være en minnepinne, en cd eller dvd, lagringsenheten i et digitalt fotoapparat eller en harddisk.

### *Eskalering av brukerrettigheter*

Formålet med å skaffe seg økte brukerrettigheter kan for eksempel være å overta kontrollen med datasystemet ved å skaffe seg tilgang til systemadministrators område. Et annet tenkelig motiv kan være å skaffe seg innsyn i en kollegas skjermede område, eller i et skjermet område på et webhotell hvor man selv allerede har brukerkonto. Inntrengning på administrators område kan ha store sikkerhetsmessige konsekvenser fordi det kan gi styringsmulighet over mange brukere og verdifulle ressurser. Men også horisontal inntrengning må anses som en alvorlig handling, blant annet fordi den krenker privatlivets fred. Også andre interesser kan rammes, for eksempel dersom brukerområdet forvalter bedriftshemmeligheter som er betrodd en spesiell medarbeider. Når man overskrider grensene for sitt brukerområde skaffer man seg tilgang til en annen «del av» datasystemet, noe som rammes av utkastet § 4.

### *Særlig om ulovlig tilgang til frittstående lagringsmedier*

Straffebudet er innholds- og teknologinøytralt. Dette følger direkte av begrepet «datasystem», som er knyttet til begrepet «data», se utkastet § 1 bokstav a, jf. bokstav c, og kommentarene i kapittel 5.2 og kapittel 9.1. Utvalget har sett det som ønskelig å samordne de forskjellige reglene som regule-

rer straffansvaret for uberettiget tilgang til data som etter gjeldende rettstilstand er spredt på forskjellige bestemmelser. Bestemmelsene er straffeloven §§ 145 annet ledd og 262 annet ledd, samt åndsverkloven § 53a første ledd, jf. § 54 første ledd bokstav b. Harmoniseringsspørsmålet er drøftet i kapittel 5.1.2.

Som det tidligere er redegjort for, innebærer praktiske tilfelle av uberettiget tilgang at det ofte må foretas et beskyttelsesbrudd. Imidlertid er den uberettigete tilgang straffbar også om datasystemet er ubeskyttet. Det har vært vanlig å anse tilgangen som en selvstendig handling som må ses atskilt fra en eventuell påfølgende tilegnelse av data eller databasert informasjon. Denne tilnærming lar seg gjennomføre for tilgang til og tilegnelse av data som er lagret. Mens det er større grad av sammenfall mellom tilgangen og tilegnelsen for så vidt gjelder data som overføres. Uberettiget tilgang til data som er lagret reguleres altså av utkastet § 4, fordi dataene befinner seg på datasystemet eller på en del av dette, mens en eventuell påfølgende tilegnelse av dataene, for eksempel ved kopiering bedømmes etter utkastet §§ 5 eller 6. For data som overføres kan det være sammenfall mellom den uberettigete tilgang og selve tilegnelsen, for eksempel ved dekoding av beskyttede fjernsynssignaler. Dette skal bedømmes etter utkastet §§ 5 og 6. Dette er også nærmere belyst i kapittel 5.5.2 i underkapitlet «Harmoniserings og konkurrensspørsmål».

Den straffbare tilgang til et datalagringsmedium (jf. «del av» et datasystem i utkastet § 4), kan bestå i at en minnepinne kobles til datamaskinen og åpnes for avlesing. Dersom innholdet er passordbelagt er tilgangen fullbyrdet når passordet er tastet inn og tilgang til innholdet gis. Dette er en variant av passordinnbrudd.

Straffbar tilgang, jf. utkastet § 4, kan også skje ved fjerning av integritetsvernet på data, for eksempel på en film lagret på en dvd-plate. Beskyttelsesbruddet (tilgangen) leder til at innholdet kan kopieres (tilegnes) og spres i ubeskyttet tilstand. Beskyttelsesbruddet eller omgåelsen, er i dag straffbar etter åndsverkloven § 53a første ledd, jf. § 54 første ledd bokstav b, for så vidt gjelder opphavsrettslig vernet materiale. Dersom materialet har annen karakter kan det ha vern etter den generelle bestemmelse i straffeloven § 145 annet ledd som omfatter «data som lagres». Selve beskyttelsesbruddet eller omgåelsen rammes av utkastet § 4, jf. «tilgang». Den uberettigete tilegnelse av innholdet rammes av utkastet §§ 5 eller 6.

Også utnyttelse av en datatape kan rammes av utkastet § 4, når den settes i en spiller og avspilling startes. Men her går det en fin grense mellom den handling som gir tilgang og selve tilegnelsen av den databaserte informasjonen, som rammes av utkastet § 5.

*Rettsstillingen til innehaveren av datasystemet*

Innehaveren av et datasystem står i en spesiell stilling fordi han har teknisk tilgangsmulighet til hele systemet. Normalt er ikke noen del av systemet absolutt stengt for ham, med mindre han selv har besluttet det og innrettet seg deretter.

Straffebudet om ulovlig tilgang til datasystem i utkastet § 4 skal verne mot inntrengning fra eksterne personer eller av brukere som overskrider den rett de er tildelt. Innehaveren *qua innehaver* omfattes ikke av denne personkretsen. Innehaverens innsynsrett kan være begrenset som følge av andre regler som for eksempel er gitt til vern for personvernet generelt, arbeidsrettslige regler om begrensninger i innsynsretten overfor arbeidstakernes data, bestemmelser i registerlovgivningen m.v. Et eventuelt innsyn foretatt av datasystemets innehaver må vurderes i forhold til de nevnte bestemmelser. Det blir ikke spørsmål om å anvende utkastet § 4 på slike tilfelle. Forutsetningen er som nevnt at et eventuelt innsyn skjer av innehaver som innehaver, det vil si at innsynet skjer i forbindelse med ivaretakelse av drift og sikker bruk av datasystemet sett i lys av det formål det skal tjene. I praksis vil innehaverens kontroll- og styringsbehov ivaretas gjennom systemadministrators funksjoner. Straffebudet om ulovlig tilgang er altså ikke ment å gjøre noen innskrenkning i systemadministrators adgang til å utøve sine oppgaver.

*Harmoniseringsspørsmål*

Som det har fremgått dekker utkastet § 4 straffeloven § 145 annet ledd for så vidt gjelder «data som er lagret». Data som overføres omfattes ikke av utkastet § 4, men av utkastet §§ 5 og 6, som blant annet rammer tapping og avlytting, se kapittel 5.5.2. Videre omfattes området for åndsverkloven § 53a første ledd, det vil si «å omgå effektive tekniske beskyttelsesmekanismer» som benyttes for å kontrollere eksemplarfremstilling eller tilgjengeliggjøring av et vernet verk. Et slikt vernet verk vil være representert på et datalagringsmedium som er «del av» et datasystem, jf. utkastet § 4.

I den grad forbudet mot uberettiget dekoding i straffeloven § 262 kan anses å gi vern for data som er lagret eller som behandles på et datasystem, dekkes også dette området av utkastet § 4. Forbudet mot

uberettiget dekoding av vernede tjenester står i straffeloven § 262 annet ledd. Vernet tjeneste er definert i bestemmelsens fjerde ledd bokstav a og b, og omfatter betalingsbelagte tilgangskontrollerte radio- og kringkastingstjenester og informasjonssamfunnstjenester. I tillegg omfattes tilgangskontrollen som sådan når den er en egen tjeneste (fjerde ledd siste punktum). Både radio- og kringkastingssignaler og de nevnte informasjonssamfunnstjenester er signaler, det vil si data, under overføring.

Når dekodingen gjelder signaler under overføring er det stor grad av sammenfall mellom dekodingen og selve tilegnelsen av signalet. Etter systematikken i lovforslaget anses dette som uberettiget tilegnelse av data under overføring, det vil si varianter av avlytting og tapping av en signalstrøm. Slike tilfeller skal bedømmes etter utkastet §§ 5 og 6.

For informasjonssamfunnstjenester som altså gjøres tilgjengelig på individuell forespørsel, kan man imidlertid tenke seg at den uberettigete dekoding kan utføres som et passordinnbrudd på selve det datasystem som lagrer de data som ordinært skal leveres på forespørsel. I så fall er det tale om et tilfelle av uberettiget tilgang til et datasystem som rammes av utkastet § 4. Denne type handling ligger i dag i grenseland mellom straffeloven § 145 annet ledd og § 262 annet ledd, og det er neppe helt klart de lege lata, hvilket straffebud som skal anvendes. I henhold til systematikken i lovforslaget hvor verken innholdets karakter eller kommersielle leveringsbetingelser har betydning for den objektive straffbarheten, er det klart at handlingen under enhver omstendighet rammes av utkastet § 4.

De tilfelle hvor dekodingen rammer beskyttelsessystemet som sådan, jf. straffeloven § 262 fjerde ledd siste punktum, reiser ingen særlige spørsmål i forhold til lovutkastet. Dersom det er tale om dekoding rettet mot data lagret på et datasystem eller et frittstående lagringsmedium som for eksempel en dvd, kommer utkastet § 4 til anvendelse. Dersom handlingen er rettet mot data under overføring kommer utkastet §§ 5 eller 6 til anvendelse. Hvis handlingen kan karakteriseres som passordknekking eller lignende, vil den være straffbar etter utkastet § 10, jf. «fremstiller» tilgangsdata.

I alle tilfelle er dekoding en omstendighet som kan gjøre handlingen grov, jf. utkastet § 18.

### 5.6.3 Datamodifikasjon

Med datamodifikasjon tenkes det på uberettigete endringer i data. Dette er handlinger som er en direkte krenkelse av integritetshensynet, se kapittel 4.6.2. Utkastet § 7 gir data et selvstendig vern mot slike endringer. Dette er nytt sammenlignet med gjeldende rett, hvor straffeloven § 291 riktignok er gitt anvendelse på tilfeller av dataskadeverk, men hvor vernet for data anses avledet av vernet for det fysiske systemet eller lagringsmediet som dataene er knyttet til. Det er det fysiske utstyret som er «gjenstand» og som er direkte vernet etter straffeloven § 291. Vernet om data følger av en anvendelse av det såkalte funksjonelle gjenstandsbegrep, se omtalen i kapittel 5.5.1. Etter utkastet § 7 er det unødvendig å anvende en slik tolkningsmetode, siden data har et direkte vern mot uberettigete endringer. Dette følger eksplisitt av ordlyden.

Utkastet § 7 første punktum rammer den som uberettiget «endrer, ødelegger, sletter eller skjuler» data. I utgangspunktet dekker alternativet «endrer» alle de øvrige alternativene, fordi hver av de nevnte handlingene forutsetter at det skrives til datasystemet og følgelig at det oppstår endringer. De øvrige alternativene er derfor inntatt av informative grunner for å klargjøre hva bestemmelsen omfatter. Databegrepet er vidt, jf. utkastet § 1 bokstav b og c, og enhver type data er omfattet av vernet etter utkastet § 7. Den straffbare endringen kan for eksempel skje i data som styrer datasystemet (nærmere bestemt i filer som inneholder dataprogrammer, såkalte programfiler), på brukerområder eller felles lagringsområder på systemet. Handlingen er fullbyrdet når endringen er foretatt. Integritetshensynet tilsier nemlig at filen skal være i den tilstand som den berettigete har bestemt. En uberettiget endring rammer påliteligheten ved at tilliten til innhold, sikkerhet og funksjonalitet svekkes. Dette er begrunnelsen for å straffbelegge selve endringshandlingen. Det stilles ikke noe krav om at endringen rent konkret leder til feilfunksjonalitet. Også en endring som rammer en sikkerhetsfunksjon på datasystemet uten at det får noen direkte betydning for funksjonaliteten, er straffbar etter utkastet § 7. Dette er i samsvar med den gjeldende rett. Straffeloven § 291 tolkes slik at den rammer uberettigete endringer selv om funksjonaliteten ikke rammes, se bakdørkjennelsen (Rt. 2004 side 1619). Se Sunde 2006 «Lov og rett i cyberspace» kapittel 6.2.2.

Om forståelsen av de forskjellige endringsalternativer som er angitt i straffebudet vises det til spesialmotivene, kapittel 9.7.

Endringer kan ha konsekvenser og det kan reises spørsmål ved hvordan slike konsekvenser strafferettslig skal bedømmes. Endringen kan for eksempel lede til at informasjon går tapt, at funksjonalitet endres dersom en programfil blir erstattet av en «logisk bombe», eller at systemet har fått tillagt nye brukerrettigheter fordi det er gjort endringer i passordfilen.

I Sunde 2006 «Lov og rett i cyberspace» side 197-198 omtales en dom av 4. november 2002 fra Skien og Porsgrunn tingrett. Saken tjener til illustrasjon av skadeverk i form av logisk bombe utført ved uautoriserte endringer i kildekode. Tiltale for grovt skadeverk var tatt ut mot en 42 år gammel mann som hadde vært

> «ansatt som programmerer i en bedrift som laget og solgte et «administrativt databehandlingsverktøy med funksjoner for regnskap, fakturering, ordre, material og produksjonsstyring». Vedkommende foretok 17 uautoriserte endringer i kildekoden i dataprogrammet. Endringene ville gi «45 avvik fra normalprosedyren i [datamaskinprogrammet] fra og med årsskiftet 2001/2002 [...]. Endringene ville påført [bedriften] og dets kunder store skader dersom de ikke hadde blitt oppdaget og utbedret i tide. Programmereren ble for dette domfelt for grovt skadeverk, jf. strl. §§ 292, jf.. 291.»

Dersom følgen er av en slik art at den kan karakteriseres som en *skade*, følger det direkte av utkastet § 18 at momentet har betydning for om lovbruddets skal anses å være grovt, jf. formuleringen «legges det særlig vekt på den skade som er voldt». Dersom endringen knapt kan sies å ha hatt betydning kan det lede til at lovbruddet anses som lite, jf. utkastet § 19 «om skadepotensialet er lite». Ellers kan karakteren av følgen ha betydning som straffutmålingsmoment.

Utkastet § 7 rammer ikke fysisk beskadigelse av datautstyr som har til følge at data skades eller går tapt. Et eksempel kan være å ripe opp en cd slik at dataene ikke lenger er lesbare. Dette er fysisk skadeverk, som rammes av en egen bestemmelse om det. Det antas at verdien av de data som gikk til spille kan ha betydning ved bedømmelsen av det fysiske skadeverket.

Det *kan* dog tenkes tilfelle som minner om fysisk skadeverk som kan rammes av utkastet § 7, dersom det gjelder skade på data som nevnt i utkastet § 1 bokstav c annet punktum, for eksempel data lagret på hullkort. Modifikasjon som rammes av utkastet § 7 kan forvoldes ved å stikke ut nye hull i eksisterende hullkort. Dette vil gi endrete eller ødelagte data. Dersom selve hullkortet ødelegges, for eksempel ved at det rives i stykker, foreligger et vanlig fysisk skadeverk.

### 5.6.4 Driftshindring

*Problemstilling*

Straffebudet om driftshindring i utkastet § 13 er nytt og rammer handlinger som går ut på å krenke tilgjengeligheten til datasystemer og elektroniske kommunikasjonsnett. Når tilgjengeligheten krenkes oppstår såkalt tjenestenekt, det vil si at kapasiteten er forbrukt eller så kraftig belastet at datasystemet eller det elektroniske kommunikasjonsnettet ikke kan utføre sine ordinære funksjoner. Det vises til kapittel 4.6.2 for en nærmere beskrivelse tilgjengelighetshensynet. I lovforslaget benyttes betegnelsen *driftshindring* om slik tjenestenekt. Vanlige betegnelser på rettsstridige handlinger som resulterer i driftshindring er tjenestenektangrep eller overbelastningsangrep.

Som det fremgår er driftshindring resultatet av en skadevoldende handling. Etter gjeldende rett rammes slike handlinger av straffeloven § 291. For disse tilfellene har det ikke vært nødvendig å anvende det funksjonelle gjenstandsbegrep ved fortolkningen, siden det nettopp er datasystemet som settes ut av drift. Det funksjonelle gjenstandsbegrep er omtalt i kapittel 5.5.1 med videre henvisninger. Det fremstår altså som en i og for seg dekkende mulighet å la driftshindring fanges opp av den alminnelige skadeverksbestemmelsen som er foreslått videreført i den nye straffeloven, jf. delutredning VII side 367, om forslag til § 29-1 om skadeverk. Overtredelsen innebærer imidlertid misbruk av datasystem og kan derfor karakteriseres som en typisk datakriminell handling som bør straffbelegges ved et straffebud som står i datakrimkapitlet i ny straffelov. Utkastet § 13 er således å anse som *lex specialis* i forhold til den alminnelige skadeverksbestemmelsen.

*Legislative hensyn*

Driftshindring kan oppstå ved bruk av forskjellige metoder. I kapittel 3.4.9 finnes en faktisk beskrivelse av disse fremgangsmåtene. Rettslig kan det være naturlig å sondre mellom driftshindring forårsaket av en ekstern handling og driftshindring som skjer innenfra, det vil si av en som allerede er berettiget til å bruke datasystemet. Videre bør det skilles mellom tilfelle hvor handlingen faktisk har resultert i driftshindring og tilfelle hvor handlingen er egnet til å resultere driftshindring, men av en eller annen grunn ikke har gjort det.

Utkastet § 13 er bygget opp rundt disse sondringene. Etter bestemmelsens første ledd rammes eksternt tjenestenektangrep, mens internt tjenestenektangrep rammes av annet ledd. Begge alternativ omfatter handlinger som faktisk har resultert i driftshindring og handlinger som er egnet til å fremkalle et slikt resultat. I tillegg omfattes det å initiere handlinger som nevnt i første ledd.

Den tekniske fremgangsmåte for eksternt tjenstenekt- eller overbelastningsangrep, jf. utkastet

§ 13 første ledd, karakteriseres ved at den baserer seg på overføring av data over det elektroniske kommunikasjonsnettet til det datasystem som er målet for handlingen. Datapakkene som overføres er for mange og/eller for ressurskrevende til at det mottakende datasystem klarer å håndtere dem. Datasystemet forbruker kapasiteten til å forsøke å håndtere datapakkene på bekostning av de ordinære prosessene på systemet. Ikke bare datasystemet, men også datalinjen inn til systemet kan anses som mål for handlingen, siden resultatet jevnlig er at all overføringskapasitet forbrukes. I begge tilfelle er konsekvensen at datasystemet ikke lenger klarer å kommunisere med omverdenen og stenges ned.

Driftshindring er skade av midlertidig karakter. Når overbelastningsangrepet opphører kan driften av datasystemet gjenopptas. Slike angrep kan imidlertid gjennomføres målrettet og presist, og det er eksempler på at de har vært gjenopptatt så snart det angrepne system er satt i drift igjen. På denne måten kan det datasystem som utsettes for angrepet settes ut av drift over lengre tid. Effekten av slike angrep kan dermed være særdeles skadelig og påføre innehaveren av datasystemet store økonomiske tap. De omfattende skadevirkningene begrunner et behov for særlig høy strafferamme, se nedenfor.

Siden skadevirkningene av overbelastningsangrep er så store bør det anses tilstrekkelig for straffbarhet at det er begått en handling som *er egnet til* å forårsake driftshindring, og legges mindre vekt på om driftshindring faktisk ble resultatet av handlingen. Anvendelse av et slikt alternativ i straffebudet vil innebære at eventuelle beskyttelsestiltak iverksatt for å forebygge driftshindring (slik at det skadelige resultatet ikke inntrer), ikke får betydning for straffeskylden.

Overbelastningsangrep kan også utføres ved å gi instrukser til et dataprogram om å iverksette et angrep på et gitt tidspunkt i fremtiden. Da har gjerningspersonen gjort alt som er nødvendig for å gjennomføre et overbelastningsangrep, og dette bør anses avgjørende for straffeskylden. Et eksempel kan være at gjerningspersonen via et program han kontrollerer har gitt agenter (maskiner som inneholder dertil egnede programmer) i et uautorisert nett (botnett) kommando om å sette i gang et overbelastningsangrep på et gitt fremtidig tidspunkt. I et slikt tilfelle kan den skadevoldende handling sies å være «initiert» og det foreslås et eget alternativ i straffebudet om dette. Den straffbare handling er dermed fullbyrdet når angrepet er tilrettelagt og automatisk vil bli utført. Det er uten betydning for straffeskylden om andre klarer å gripe inn og forhindre at angrepet faktisk utløses eller iverksettes. Dersom gjerningspersonen selv trekker kommandoen tilbake kan straffeloven § 59 om nedsettelse av straff eller anvendelse av mildere straffart komme til anvendelse, sml. ny straffelov § 80 bokstav a nr. 1. Et angrep kan også anses initiert når den som kontrollerer et botnet gir angrepskommando i samtid.

Tilsvarende betraktninger gjør seg gjeldende for overbelastningsangrep som skjer innenfra ved at en som er berettiget til bruk av datasystemet, rettsstridig iverksetter prosesser som er så kapasitetskrevende at det oppstår driftshindring. Et eksempel kan være at en ansatt i en bedrift starter opp et såkalt bakterieprogram som ikke har noen annen funksjon enn å restarte seg selv. Etter hvert vil dataprogrammet forbruke hele maksinkapasiteten til dette på bekostning av de ordinære prosesser på systemet. Datasystemet vil dermed også bli satt ut av stand til å kommunisere med omverdenen. Denne type driftshindring foreslås gjort straffbart, jf. utkastet § 13 annet ledd.

Det anses tilstrekkelig at handlingen er egnet til å skape driftshindring. Begrunnelsen er den samme som for første ledd nevnt ovenfor, det vil si at det ikke bør ha relevans for straffespørsmålet om innehaveren av datasystemet klarer å iverksette tilstrekkelige beskyttelsestiltak.

#### *Konkurrensspørsmål*

De tekniske fremgangsmåter for å skape driftshindring kan variere: Med mindre overbelastningen skapes ved en metode som er absolutt ekstern, vil handlingene innebære et element av rettsstridig datatilførsel og rettsstridig bruk av datasystemet. Med absolutt ekstern fremgangsmåte menes at det utelukkende er tale om ytre påvirkning på dataystemets prosesser, eller på det elektroniske komunikasjonsnettverkets kapasitet.

Overbelastningsangrep kan imidlertid utføres ved å tilføre datasystemet datapakker som er av en slik art eller størrelse at operativsystemet ikke klarer å håndtere det, noe som som resulterer i datakrasj. Metoden Ping of Death er eksempel på dette, se kapittel 3.4.9. Det kan reises spørsmål ved om denne tilførselen av datapakker inn i det system som er mål for handlingen, også er datamodifikasjon, jf. utkastet § 7, ved at det rettsstridig tilføyes data til dem som allerede ligger på systemet. Den direkte konsekvens av datatilførselen er at datasystemet slutter å fungere på grunn av den rettsstridige påvirkningen på operativsystemet. Når datasystemet startes opp på nytt er de skadelige datapakkene forsvunnet og utgjør dermed ikke noen

endring som sådan på datasystemet. Det oppstår ikke spørsmål om konkurrens med utkastet § 7 i et slikt tilfelle. Men dette stiller seg annerledes dersom det tas i bruk en metode for driftshindring som på mer varig måte etterlater fremmede data med skadelig funksjonalitet på datasystemet. Dette vil i så fall kunne anses som datamodifikasjon i tillegg til driftshindring.

En regel om straff for driftshindring forårsaket internt har først og fremst som formål å ramme tilfeller hvor gjerningspersonen i utgangspunktet har rett til å programmere, installere eller starte opp nye dataprogrammer på datasystemet. Hvis vedkommende mangler slik rett vil introduksjon og bruk av et fremmed program etter omstendighetene kunne anses som datamodifikasjon og ulovlig bruk, jf. utkastet §§ 7 og 8. Er resultatet av handlingen tjenestenekt uten at dette var omfattet av forsettet, eller kan anses som grovt uaktsomt, er det en skjerpende omstendighet som kan lede til at lovbruddet anses å være grovt, jf. utkastet § 18 «den skade som er voldt», og det er uansett et skjerpende moment ved straffutmålingen.

Dersom gjerningspersonen programmerer, installerer eller starter opp et dertil egnet program med forsett om å skape driftshindring, eller er grovt uaktsom i så henseende, kommer utkastet § 13 annet ledd til anvendelse. Hvorvidt et slikt program i utgangspunktet er å anse som et fremmedeelement som utgjør en datamodifikasjon, jf. utkastet § 7, avhenger av omstendighetene og må følgelig vurderes konkret. Dersom det er tale om en programmerer som har frihet til å programmere og kjøre nye programmer, kan straff for driftshindring tenkes uten at det nødvendigvis også foreligger en overtredelse av utkastet § 7 om datamodifikasjon. Det forutsettes da at programmet ikke har andre skadelige egenskaper enn å stjele kapasiteten på systemet. Hvis det også endrer eller sletter data skal forsettlig oppstart av programmet naturligvis rammes av utkastet § 7. En slik bruk av datasystemet vil også i seg selv være rettsstridig og rammes av utkastet § 8. I tillegg kan det være aktuelt å vurdere befatningen med det skadelige dataprogrammet opp imot vilkårene i utkastet § 11.

Til slutt antas det at et straffebud om driftshindring kan anvendes i konkurrens med straffeloven § 151 b eller et tilsvarende straffebud i ny straffelov. Det vises til at mens straffeloven § 151 b først og fremst har vern om allmenne interesser for øye, er straffebudet om driftshindring satt til vern om innehaverens interesse i et velfungerende uskadet datasystem. Indirekte er dette selvfølgelig også i samfunnets interesse, men det primære etter utkastet § 13 er likevel vernet om eierinteressene i datasystem og elektroniske kommunikasjonsnett.

*Strafferammer*

Driftshindring kan som nevnt utføres presist ogt målrettet, og har skadelige konsekvenser ofte i form av meget store økonomiske tap. Dersom det datasystem eller elektroniske kommunikasjonsnett som rammes tilhører en stor bedrift eller forestår prosesser som er viktige for samfunnet mer generelt, kan handlingen få preg av sabotasje. Anvendeligheten av sabotasjebestemmelsen i straffeloven § 151 b antas imidlertid å være noe uavklart når målet for handlingen er en privat bedrift, selv om det i og for seg er tale om virksomhet som har stor betydning. Det antas da at vilkåret om å forvolde en «omfattende forstyrrelse» ikke så lett vil være oppfylt. Utvalget går derfor inn for å anvende en streng strafferamme i utkastet § 13 med tanke på de alvorligste tilfellene av driftshindring, også om de ikke kan karakteriseres som «sabotasje». Den ordinære strafferammen foreslås satt til bøter eller fengsel inntil 6 år. Ved grov overtredelse øker strafferammen til fengsel inntil 10 år. Dette er strengere enn etter gjeldende strafferamme for grovt skadeverk, som er på fengsel inntil 6 år, jf. straffeloven § 292, og på linje med strafferammen på 10 år i sabotasjebestemmelsen i straffeloven § 151 b.

### 5.6.5 Uberettiget bruk av datasystem

*Problemstilling og forslag til straffebud*

Utvalget foreslår en bestemmelse om uberettiget bruk av datasystem, jf. utkastet § 8 første ledd. Etter første punktum straffes den som «uberettiget benytter andres datasystem eller elektroniske kommunikasjonsnett». Annet punktum inneholder en presisering av rettsstridsreservasjonen når bruken gjelder «et tilgangspunkt til internett i usikret trådløst elektronisk kommunikasjonsnett».

Utkastet § 8 vil være en videreføring av de gjeldende bestemmelser i straffeloven §§ 261 og 393 om uberettiget bruk av løsøregjenstand, når bruken gjelder datasystemer. Straffelovkommisjonen har foreslått å videreføre straffeloven §§ 261 og 393 i kapittel 30 om tyveri, underslag, ran, utpressing m.v, jf. § 30-14 ulovlig bruk av løsøregjenstand og § 30-15 om grov ulovlig bruk av løsøregjenstand. Det vises til delutredning VII side 373. Utvalgets forslag til straffebud om ulovlig bruk av datasystem, er en spesialregel i forhold til de nevnte straffebud i delutredning VII.

Straffeloven § 261 ble tatt inn i forbindelse med styrkingen av vernet mot datakriminalitet i 1987. Vernet om datasystemer fremgår ikke direkte av ordlyden, som er utformet som et generelt forbud mot misbruk av «løsøregjenstand». Det kreves også at bruken har påført den berettigete «betydelig vinning eller betydelig tap». Det er særlig forseelsesbestemmelsen i § 393, som bare krever «Tab eller Uleilighed», som har vist seg praktisk anvendelig i forbindelse med datakriminalitet. Med unntak for en såkalt «tellerskritt-dom» i Rt. 1989 side 980, ses ikke straffeloven § 261 å ha blitt forsøkt anvendt i forbindelse med datakriminalitet (i den nevnte dom ble forholdet nedsubsumert til straffeloven § 393). Dette antas å ha sammenheng med problemet med å kvantifisere vinning eller tap ved uberettiget bruk av datasystem.

Utvalgets utgangspunkt er at eierrådigheten gir rett til å sette regler for bruken av et datasystem. Selve datasystemets formål kan også gi visse rammer for bruken, uten at formålet nødvendigvis er nedfelt i noen instruks. Dette må vurderes konkret. Brytes slike regler, enten de er fastsatt eksplisitt eller følger implisitt av formål eller situasjon, vil bruken kunne anses som rettsstridig og følgelig kunne rammes av utkastet § 8. Bestemmelsen er således særlig begrunnet i behovet for vern om eierens eller den berettigedes økonomiske interesse i datasystemet, typisk en bedrifts investering i sitt datasystem. Det vil da gjelde visse regler og forutsetninger for bruken, som skal respekteres av brukerne. Den samme begrunnelsen lå til grunn for innføringen av regelen om uberettiget bruk av løsøregjenstand i straffeloven § 261 i 1987, se NOU 1995: 31 særlig på side 30 første spalte.

Vernet gjelder ressursene på datasystemet, det vil si kapasitet og funksjonalitet. Overtredelse kan derfor foreligge selv om utnyttelsen i det enkelte tilfelle gjelder ordinære tjenester på systemet. Det er ikke en betingelse for straff at det settes i gang ulovlige prosesser, for eksempel i form av installering av avlyttingsutstyr eller lignende. Slike handlinger vil regulært rammes av andre bestemmelser i lovforslaget, særlig utkastet § 7 om datamodifikasjon. Det avgjørende i forhold til utkastet § 8 er om bruken kan karakteriseres som uberettiget.

Utvalget går ikke inn for å anvende noe krav i utkastet til § 8 om at den rettsstridige bruken skal lede til vinning, tap eller uleilighet. Dette er en endring i forhold til de vilkår som stilles etter straffeloven §§ 261 og 393. Etter ordlyden i utkastet § 8 kreves det altså mindre for at bruken skal være straffbar enn etter de gjeldende straffebud. Denne endringen i ordlyden innebærer likevel ikke noen realitetsendring med hensyn til terskelen for straff, siden det vanskelig kan tenkes tilfeller av ulovlig bruk som ikke i det minste innebærer «uleilighet» for den berettigete, sammenlign vilkåret i straffeloven § 393. Dessuten er formuleringen av utkastet § 8 hensiktsmessig for å kunne ramme tilfeller av misbruk som er rettet mot mange, men hvor den individuelle konkrete uleilighet er vanskelig å dokumentere for eksempel fordi ofrene er i utlandet. Saksforholdet i bakdørkjennelsen (Rt. 2004 side 1619) er illustrerende i så måte. De to gjerningspersonene hadde installert «bakdør» på 437 datasystemer verden over. Det synes rimelig å kunne ramme dette etter regelen om ulovlig bruk. For så vidt gjelder vilkåret vinning (sammenlign straffeloven § 261), så gjøres dette rettslig relevant ved vurderingen av om lovbruddet er grovt, jf. utkastet § 18.

### *Hva som menes med «bruk», jf. utkastet § 8*

Med «bruk» etter utkastet § 8, menes faktiske handlinger, ikke rettslige disposisjoner. «Bruk» omfatter handlinger som retter seg mot prosessene, tjenestene og kapasiteten på datasystemet, herunder alle dets komponenter. Straffebudet kan for eksempel ramme en arbeidstakers bruk av arbeidsgiverens datasystem til å laste ned musikkfiler fra internett. Det er ikke noe vilkår at nedlastningen er ulovlig etter andre regler, for eksempel etter åndsverklovens bestemmelser. Avgjørende for straff etter utkastet § 8 er at bruken må anses uberettiget i forhold til det datasystem som er utsatt for handlingen. I det nevnte eksempel kan derfor bruken tenkes å være uberettiget og straffbar etter utkastet § 8 selv om nedlastningen av musikkfilene er lovlig, for eksempel fordi arbeidstakeren laster ned fra en lovlig betalingstjeneste (nettbutikk). Se nærmere om rettsstridsreservasjonen nedenfor.

Det er uten betydning om nedlastingen i et slikt tilfelle skjer til harddisken på datasystemet, eller til en lagringsenhet som senere benyttes på andre systemer, for eksempel til en cd-rom eller en mp3-spiller. Overføringen til lagringsmediet skjer når den er tilkoblet eller installert i datasystemet, og er følgelig en del av dette når bruken skjer.

Som det har fremgått, er nedlastingen og kopieringen (lagringen) programstyrte prosesser som initieres og utføres på datasystemet, og dette innebærer altså «bruk» i utkastet § 8 sin forstand. Ordet «bruk» omfatter derimot ikke fysiske handlinger som bare gjelder utstyret, for eksempel det å uberettiget ta med seg bedriftens datautstyr hjem. Her kan reglene om tyveri og underslag komme til anvendelse. I tillegg kan bestemmelser

om uberettiget bruk av løsøregjenstand være aktuelle, for eksempel der bruken gjelder lagring til en harddisk eller minnepinne som kan gjenbrukes for å lagre, endre eller slette data.

Andre eksempler på «bruk», jf. utkastet § 8, kan være å misbruke en annens datasystem for å etablere et uautorisert nett (botnett). Bruken av systemet (datamaskinen som agent) er ulovlig bruk, jf. utkastet § 8. Selve installeringen av programmet som muliggjør dette kan straffes som datamodifikasjon, jf. utkastet § 7. Tilsvarende vil et misbruk av en annens datasystem for utsending av spam, jf. utkastet § 14, være «bruk», jf. utkastet § 8.

*Rettsstridsreservasjonen*

*a) Innledning*

Avgjørende for straff er at det er tale om bruk som er «uberettiget». Det er meningen at utkastet § 8 både skal ramme bruk som skjer av eksterne personer som er helt uberettiget til å anvende systemet, og av brukere som er berettiget til å benytte systemet, men som bruker det på ulovlig måte. I det første tilfellet kan det for eksempel være tale om en som har logget seg på med et stjålet passord og deretter utnytter systemet. I det andre tilfellet kan det være tale om bruk i strid med retningslinjer som er kommunisert til brukeren på tilfredsstillende vis.

*b) Bruk utført av eksterne personer*

Bruk som skjer av eksterne, det vil si personer som i utgangspunktet mangler rett til å skaffe seg tilgang til systemet, vil være rettsstridig etter utkastet § 8, i tillegg til at handlemåten vil kunne være straffbar etter utkastet § 4. I denne kategorien faller også bruk som skjer på grunnlag av gamle tilgangsrettigheter som fremdeles lar seg utnytte på systemet. Det vises til omtalen av denne problemstillingen i kapittel 5.6.2.

Straffebudet i utkastet § 8 første ledd annet punktum kommer imidlertid inn som en praktisk begrensning av rettsstridsvilkåret for eksterne brukere. Bestemmelsen lyder:

Bruk av andres tilgangspunkt til internett i usikret trådløst elektronisk kommunikasjonsnett anses ikke som uberettiget.

Som det fremgår av ordlyden tas det her sikte på å klargjøre rettstilstanden for bruk av usikret trådløst nettverk for å skaffe seg tilgang til internett. Slik tilgangsmulighet tilbys ofte som en service til gjester på hotell og kafé, eller på andre møte- eller transittplasser som i resepsjonen i et forretningsbygg, på bibliotek, i kinoresepsjoner og på flyplasser. I slike tilfeller reiser det seg åpenbart ikke noe spørsmål om berettigelsen av å bruke tjenesten, den er helt klar.

I annen sammenheng kan det imidlertid herske noe tvil om retten til å benytte et usikret nett. Spørsmålet oppstår når slik tilgang er mulig nettopp fordi nettet er åpent tilgjengelig («usikret»), men man ikke kan vite om tilgangen er ment for det alminnelige publikum. I praksis er det ofte mulig å benytte privatpersoners bredbåndstilknytning til internett, fordi det ikke er satt opp noen sperre mot slik bruk. Årsaken kan være at vedkommende har glemt å sikre seg, men det kan også være at vedkommende ønsker å dele internettilgangen med andre.

Forutsetningen for drøftelsen er at bruken er begrenset til å gjelde tilgang til internett. Problemstillingen inviterer ikke til å vurdere om det kan være berettiget å skaffe seg tilgang til internettabonnentens datasystem via det usikrede nettet. En slik handling rammes uansett av utkastet § 4.

Men for tredjepersons bruk av internettilgangen kan det pekes på at slik tilgang enkelt oppnås fordi bærbare datasystemer har funksjonalitet for automatisk å søke og koble seg opp dersom slike nett først er tilgjengelige. Bak dette ligger tilgjengelighets- og effektivitetshensyn. Det skal være enkelt å koble seg til internett fordi det letter kommunikasjons- og samhandlingsmulighetene i samfunnet generelt. Videre tilsier samfunnsøkonomiske hensyn at nettverksressurser utnyttes så effektivt som mulig. En tredjepersons bruk av et usikret nett vil normalt ikke gå ut over internettabonnentens egen bruk. Effektivitetshensyn taler derfor mot at slik bruk kriminaliseres.

Disse hensyn gjelder bare for usikrede nett. Dersom nettet er tilgangskontrollert vil en tredjepersons bruk være uberettiget. Selve handlemåten som går ut på å skaffe seg tilgangen vil i et slikt tilfelle være straffbar etter utkastet § 4.

Overfor regelen i utkastet § 8 første ledd annet punktum, kan det innvendes at det gir en fare for at internettabonnenten identifiseres med tredjepersons aktiviteter på internett. Dersom den eksterne person begår ulovlige eller kritikkverdige handlinger på internett vil mistanken i første omgang rette seg mot internettabonnenten (sluttbrukeren), fordi det er IP-adressen til vedkommendes datasystem som vises som oppkoblingspunkt på internett. Omverdenen vil ikke i utgangspunktet kunne vite at handlingen utføres av en annen enn internettabonnenten.

Utvalget mener at dette hensynet ikke kan være avgjørende for utformingen av rettsstridskravet. Det er vanlig at et datasystem benyttes av en

annen enn den som står som internettabonnent. Det kan være husstandsmedlemmer (mor eller far står som abonnent), arbeidstakere (bedriften står som abonnent), beboere i et borettslag (styreformannen eller borettslaget står som abonnent). Følgelig kan man neppe ta som alminnelig utgangspunkt at den som er registrert som abonnent også er den som faktisk har utfoldet seg på internett. Hvem dette er må undersøkes konkret. Dette er en selvsagt forutsetning ved etterforsking av internettkriminalitet. Det er heller ikke grunn til å tro at vanlige internettbrukere baserer seg på opplysninger om IP-adresse når de kommuniserer i sammenhenger hvor personrelasjonen har betydning. Ved slik kommunikasjon er det andre opplysninger som vektlegges, blant annet former for sikker kommunikasjon (autentisering) og opplysninger som fremgår av innholdet i kommunikasjonen.

Til slutt har internettabonnenten mulighet til å sikre seg teknisk og kan få profesjonell assistanse til dette. I så fall vil han være beskyttet mot tilgang og bruk av tilgangspunkt til internett, både etter utkastet §§ 4 og 8.

### *c) Bruk utført av personer med rettmessig tilgang til datasystemet*

For så vidt gjelder bruk av datasystemet av brukere som har rettmessig tilgang, er det hensiktsmessig å inndele spørsmålet om rettsstrid i forskjellige kategorier. For det første er det tale om bruk som er ulovlig etter andre straffebestemmelser, for eksempel forbudet mot befatning med seksualiserte skildringer av barn, jf. straffeloven § 204a. Bruk av datasystemet til et slikt formål vil både være en krenkelse av straffeloven § 204a og av utkastet § 8, fordi utnyttelsen av en annens datasystem til et slikt formål under enhver omstendighet er uberettiget med mindre eieren har samtykket. Straffebudene skal følgelig anvendes i konkurrens.

Videre kan det være tale om bruk til et formål som isolert sett er lovlig, men som blir uberettiget fordi bruken faller utenfor datasystemets formål, eller regler satt for bruken. Formålet kan fremgå av retningslinjer eller av situasjonen. Dette må avgjøres konkret. Dersom det er tale om utnyttelse av arbeidsgivers datasystem er utgangspunktet at bruken skal være arbeidsrelatert, med mindre det er gitt tillatelse til annen bruk. «Annen bruk» kan være av meget ulik karakter, noe som medfører at handlemåten i visse tilfeller kan være uberettiget, jf. utkastet § 8, mens den i andre tilfeller er innenfor det akseptable.

Privat bruk av arbeidsgivers datasystem kan være uberettiget. Arbeidsgiver må anses å ha stor frihet i å utforme retningslinjer for bruken. Det kan også gjelde ulike retningslinjer for ulike deler av datamaskinparken i en bedrift. Slike retningslinjer skal overholdes såframt de er tilstrekkelig kommunisert til medarbeiderne. I tillegg må arbeidsgiver opptre slik at det er tydelig at retningslinjene tas alvorlig. Dette ble understreket i den såkalte ConocoPhillipsdommen (Rt. 2005 side 518). Her ble avskjed av to medarbeidere som hadde brukt datasystemet i strid med arbeidsgivers retningslinjer, kjent ugyldig, blant annet med henvisning til at arbeidsgiveren hadde sett mellom fingrene med den type overtredelse det var tale om.

Dersom retningslinjene ikke sier noe om adgangen til privat bruk må det antas å foreligge kutyme for dette, forutsatt at det ikke er til ulempe for bedriften og holdes innenfor et rimelig omfang. Som eksempel må det være akseptabelt å håndtere privat e-post med tilgang fra arbeidsgivers system og bruke arbeidsgivers telefon til private samtaler. Den nærmere vurdering av rettsstridskriteriet må følge arbeidsrettslige regler.

I andre tilfeller er rettsstriden mer åpenbar, for eksempel dersom arbeidsgivers datautstyr utnyttes til bruk i konkurrerende virksomhet. Det kan være tale om arbeidstakerens egen næringsvirksomhet, slik at bruken fremstår som en type «butikk i butikken»-tilfelle. Forutsetningen er selvsagt at bruken ikke er bekjentgjort overfor arbeidsgiver og at arbeidsgiver har akseptert denne.

Databruken beskrevet i Oslo tingretts dom av 10. mars 2005 (TOSLO-2004-84792), ligger lenger ut på skalaen og må klart anses som uberettiget, jf. utkastet § 8. Det vises til saksfremstillingen gjengitt i kapittel 5.5.1. Her skjedde databruken som besto i omfattende kopiering fra en bedriftsserver og overføring ved hjelp av e-posttjenesten, som ledd i et datatyveri til bruk for en konkurrent av arbeidsgiveren. Slik bruk er klart rettsstridig og straffbar, jf. utkastet § 8.

Til slutt – og uavhengig av om bruken har forbindelse med noe arbeidsforhold eller ikke – dersom bruken, slik den arter seg rent konkret, påfører datasystemet sikkerhetssvikt eller belastninger som går ut over funksjonaliteten, for eksempel fordi prosessene er for kapasitetskrevende, kan bruken etter omstendighetene anses som rettsstridig. Dette kan blant annet ha betydning i forbindelse med uttesting av ukjente programmer på datasystem man ikke har tillatelse til å bruke for slikt formål. Det innebærer en risiko å teste ukjente programmer. Programmet kan vise seg å

ha egenskaper som skader systemet. Testvirksomhet uten tillatelse kan derfor i seg selv være en aktivitet som kan anses som rettsstridig etter utkastet § 8. Dette gjelder selvsagt ikke dersom slik testing inngår som ledd i brukerens oppgaver og testing utføres på et nærmere angitt system som kan benyttes for formålet, og innenfor de retningslinjer som er gitt.

De såkalte «tellerskrittsakene» har vært subsummert under reglene om rettsstridig bruk, jf. straffeloven §§ 261 og 393, og etter reglene om uberettiget tilgang i konkurrens med databedragеribestemmelsen, jf. straffeloven § 145 annet ledd jf. § 270 første ledd nr. 2. Det vises til Rt. 1989 side 980 og Rt. 1992 side 790 (rettsstridig bruk), og Rt. 1995 side 1872 (pinkodekjennelsen) som ble subsummert som datainnbrudd i kombinasjon med databedrageri. Subsumsjonen må nødvendigvis avhenge av fremgangsmåten som er benyttet i det enkelte tilfellet. «Tellerskrittsaker» er en merkelapp som på en gruppe handlinger som ikke nødvendigvis skal subsummeres likt. Det vises til omtalen av dette i kapittel 5.8.7.

### 5.6.6 Masseutsendelse av elektronisk kommunikasjon («spam»)

*Problemstilling*

Spam er elektroniske meldinger som masseutsendes til mottakere som verken har bedt om eller gitt forhåndssamtykke til mottak av slike meldinger. Slike meldinger representerer en stor kostnad og en teknisk belastning i kommunikasjonsnettene. Meldingene svekker påliteligheten til e-posttjenesten på flere måter, og utgjør en sikkerhetsrisiko mer generelt siden de også benyttes til å spre skadelig dataprogram som for eksempel orm og virus.

Det vises til fremstillingen i kapittel 3.6 om egenskaper og skadevirkninger av spam.

I OECD-rapporten Anti-Spam Toolkit of Recommended Policies and Measures av 13. april 2006, er effektive regelbaserte sanksjoner fremhevet som et nødvendig virkemiddel mot spam. Utvalget foreslår at det tas inn et eget straffebud mot spam i datakrimkapitlet i den nye straffeloven, jf. utkastet § 14.

*Gjeldende rett*

Straffeloven inneholder ingen bestemmelser om spam, men spam som sendes i næringsvirksomhet uten mottakers forutgående samtykke, eller i eksisterende kundeforhold, er straffbart etter markedsføringsloven § 2b, jf. § 17. Bestemmelsen gjelder bare utsendelse til fysiske personer. Det innebærer at det ikke gjelder noe forbud mot spam som sendes til bedrifter, forvaltningen, organisasjoner osv. Denne bestemmelsen foreslås videreført i utkast til § 6-2 i forslaget til ny markedsføringslov sendt på høring av Barne- og likestillingsdepartementet 7.7.2006. Markedsføringslovens forbud mot spam bidrar blant annet til å gjennomføre kommunikasjonsverndirektivet (direktiv 2002/58/EF) i norsk rett.

Ekomloven inneholder ingen regler rettet mot utsendere av spam. Imidlertid inneholder loven visse regler som kan hjemle tiltak iverksatt av tilbydere av elektronisk kommunikasjonsnett, -tjeneste, tilhørende utstyr og installasjoner, rettet mot spam. Grunnlaget er først og fremst ekomloven § 2-3 som gir Post- og teletilsynet kompetanse til å stille krav knyttet til kvaliteten og tilgjengeligheten til de nevnte nett og tjenester. Tilbyderne kan pålegges å iverksette tiltak for å nå disse kriteriene, og det antas at dette også omfatter tiltak rettet mot spam. Samferdselsdepartementet har imidlertid foreslått en presisering i den nevnte bestemmelsen i ekomloven, for å sørge for at det kommer klart frem at bestemmelsen kan brukes til dette formålet. Det vises til forslag om endringer i ekomloven og ekomforskriften sendt på høring 21. august 2006. Samferdselsdepartementet har også signalisert at det i samarbeid med Post- og teletilsynet vil følge utviklingen nøye, og fortløpende vurdere behovet for tiltak mot spam.

Ekomloven pålegger også tilbyderne å tilby nødvendig sikkerhet for brukerne, jf. § 2-10. Bestemmelsen gir myndighetene hjemmel til å pålegge tilbyderne å innføre bestemte sikkerhets- og beredskapstiltak. Etter ekomforskriften § 8-1 er forpliktelsene begrenset til tilbydere som leverer elektronisk kommunikasjonstjeneste, overføringskapasitet eller samtrafikk til bruker med samfunnskritisk funksjon, det vil si bare et begrenset utvalg av tilbydere.

Som nevnt er grunnlaget for spam ofte adresselister som er benyttet i strid med personopplysningsloven. Etter definisjonen av personopplysning i personopplysningsloven § 2 nr. 1, antas det at en e-postadresse må anses som en personopplysning når den direkte eller indirekte kan identifisere en enkeltperson, for eksempel ved at den inneholder hele eller deler av vedkommendes navn. Når en e-postadresse er å anse som en personopplysning, vil personopplysningsloven § 11 første ledd, bokstav a jf. § 8, stille krav om at det foreligger et rettslig grunnlag før e-postadressen kan benyttes for utsendelse av e-post. Ved utsendelse av spam vil et slikt rettslig grunnlag som hovedregel mangle, og utsendelsen medfører dermed brudd på person-

opplysningslovens bestemmelser. Det er per i dag ikke straffbart å handle i strid med disse bestemmelsene. Personopplysningsloven § 26 pålegger den som sender ut meldinger inneholdende direkte markedsføring å oppdatere sitt adresseregister mot et sentralt reservasjonsregister der personer som ikke ønsker å motta direkte markedsføring kan reservere seg. Brudd på denne oppdateringsplikten er straffbelagt, men har liten selvstendig betydning all den tid markedsføringsloven § 2 bokstav b krever forutgående samtykke ved utsendelse av spam i næringsvirksomhet.

*Utvalgets forslag*

Utvalget mener at problemene med spam er så omfattende og veldokumenterte at det er behov for et eget straffebud om dette. Et slikt forbud foreslås inntatt i datakrimkapitlet i den nye straffeloven, jf. utkastet § 14. Denne bestemmelsen vil altså bidra til at Norge fortsatt gjennomfører forpliktelsene i kommunikasjonsverndirektivet nevnt ovenfor.

Dagens forbud i markedsføringsloven § 2 b, jf. § 17, som foreslås videreført i den nye markedsføringsloven § 6-2, anses ikke å være tilstrekkelig, siden forbudet er begrenset til å gjelde spam som sendes «i næringsvirksomhet» hvor mottaker er en fysisk person. Tiltakene hjemlet i ekomloven er heller ikke tilstrekkelige siden de bare kan rettes mot tilbyderne, ikke de som står bak selve utsendelsen. Det er avsenderne av spam det er behov for å ramme med straff.

Skadevirkningene av spam gjør seg gjeldende generelt, uavhengig av hvem som er avsender eller mottaker eller formålet med meldingen. Det tenkes på belastningen i nettet, kostnadene som forvoldes på grunn av de sikkerhetstiltak det er behov for å ta i bruk, svekkelsen av påliteligheten til kommunikasjonstjenestene, pr. i dag særlig for e-post, og forbruket av tid som medgår til å håndtere problemet. Spam anses også å utgjøre en krenkelse av det private rom, det vil si retten til å bli latt i fred. Dette er virkninger som tilsier at et straffebud bør ramme enhver avsender av spam, uansett om det er tale om næringsvirksomhet, offentlig, privat eller for eksempel ideell eller politisk virksomhet. Et forbud mot spam anses også å støtte opp under EMK artikkel 8.

Utvalget har vurdert hvorvidt et forbud mot spam vil kunne krenke vesentlige kryssende interesser som også er viktige i et demokratisk samfunn. Det tenkes her særlig på forholdet til ytringsfriheten, siden det ligger i sakens natur at spamforbudet vil kunne utløse straffansvar for formidling av ytringer. Straffansvaret er imidlertid ikke knyttet opp til ytringens natur. Forbudet er således ikke-diskriminerende sett i forhold til ytringens innhold. Det avgjørende er måten ytringen er fremsatt på. Det antas at ytringsfriheten ikke kan påberopes som grunnlag for en rett til å formidle ytringer helt uavhengig av omkostningene og ulempene ved formidlingsmetoden. Den sentrale begrunnelsen for forbudet mot spam er at det går ut over sikkerheten ved de kommunikasjonstjenester som anvendes, og på sikt undergraver effektiviteten av disse. Dette kan ikke ytringsfriheten legitimere. Dessuten krysses ytringsfriheten av retten til privatlivets fred, som også er en grunnleggende menneskerettighet.

Utvalget er ikke kjent med at det foreligger rettspraksis fra menneskerettighetsdomstolen (EMD) vedrørende spam, men antar at det er vesentlig om et forbud åpner for at masseutsendelse likevel i visse tilfeller kan være lovlig. Det antas at en adgang til å samtykke til å motta spam (en såkalt «opt-in» klausul) kan være vesentlig i forhold til EMK artikkel 10. Det foreslås derfor at spamforbudet i utkastet § 14 uttrykkelig unntar meldinger det er samtykket til. Presiseringen antas også å være nødvendig for å få frem at mottakers samtykke går foran tilbydernes interesse i å unngå spam, som gjør seg gjeldende med like stor styrke uavhengig av om det er samtykket til meldingen eller ikke.

Her kan det være naturlig å nevne at masseutsendelse av elektroniske meldinger ikke kan sammenlignes med det å akseptere annonser eller andre oppslag i aviser og tidsskrifter, entes disse er papirbasert eller elektroniske. I slike tilfeller foreligger en aksept ved at man har skaffet seg eksemplaret eller stilt seg som abonnent til tjenesten, og da er det implisitt også samtykket til mottak av det ikke-redaksjonelle stoffet. Dette er ikke tilfelle for spam, som sendes ubedt av mottakeren.

Ytterligere antas det at rekkevidden av spamforbudet ikke bør være så vid at den rammer bruk av meldinger i eksisterende relasjoner, for eksempel for å drive kundepleie, kommunikasjon til medlemmer i en forening, fra offentlige institusjoner til borgerne m.v. Utkastet § 14 første ledd annet punktum inneholder derfor en reservasjon for dette. Formuleringen i markedsføringsloven § 2 b første ledd tredje punktum er tatt som utgangspunkt for reservasjonen i utkastet § 14. Det antas at praksis knyttet til markedsføringslovens bestemmelse, også vil kunne ha betydning for rekkevidden av utkastet § 14. Det er for eksempel ikke rettsstridig å sende invitasjoner til større private selskaper og lignende per e-post.

I tillegg til de nevnte tilfelle hvor bruk av masseutsendelse anses å være rettmessig kan det fremholdes at et spamforbud ikke innebærer noe forbud mot å ytre seg til mange adressater ved bruk av elektronisk kommunikasjon, som skjer ved andre fremgangsmåter. Flere internettjenester er tilrettelagt for å ytre seg til mange («hele verden»), for eksempel ved bruk av hjemmesider, dertil egnede news-grupper, åpne pratekanaler m.v. Også på denne måte er formidlingsretten innen ytringsfriheten ivaretatt.

Som nevnt anser utvalget at det avgjørende for straff er at det foreligger en masseutsendelse. Det er ikke hensiktsmessig å knytte forbudet opp til et vilkår om at det sendes i næringsvirksomhet. For det første kan det ofte være tvilsomt om avsender driver næringsvirksomhet i lovens forstand. Ikke sjelden inngår spam som forberedelse til bedragerier eller som ledd i annen ulovlig virksomhet, se kapittel 3.6. Dette styrker begrunnelsen for straff, men tilfellene vil falle utenom straffebudet dersom det tar i bruk et vilkår om næringsvirksomhet. Skadevirkningene gjør seg som nevnt gjeldende uavhengig av hvem som sender meldingene og hva de inneholder.

En masseutsendelse er en utsendelse som bærer noen eller alle de karakteristika som det er redegjort for innledningsvis i kapittel 3.6. Utvalget har vurdert om det er hensiktsmessig at lovteksten tallfester en minimumsgrense for antall meldinger som er nødvendige for å anse kommunikasjon som en masseutsendelse. En tallfesting vil være klargjørende, men på den annen side kan det lede til at for stor vekt legges på antallet i seg selv, mens det som nevnt er en helhetsvurdering som skal foretas. For eksempel dersom adresselister er benyttet i strid med personvernlovgivningen kreves det mindre med hensyn til antallet, enn dersom adressegrunnlaget i utgangspunktet er lovlig. Det viktigste er uansett at det er tale om en melding som sendes til mange mottakere uten at de på forhånd har samtykket til det. En annen innvending imot tallfesting er at det ikke har latt seg gjøre å identifisere en klar oppfatning om hva som skal til. En slik tallangivelse må derfor fastsettes nokså vilkårlig, noe utvalget finner lite ønskelig. Uansett skal det som nevnt foretas en totalvurdering av situasjonen. Det vises også til de spesielle merknadene i kapittel 9.14 om dette.

Utvalget mener som nevnt at det er hensiktsmessig å overføre spamforbudet til straffeloven, fordi det knytter seg langt flere interesser bak forbudet enn de forbruker- og markedsføringsrettslige interessene. Dette gjenspeiles i ordlyden til utkastet § 14 som rammer masseutsendelse generelt, med visse unntak som nevnt. Disse unntakene er imidlertid ikke knyttet til noen spesielle interesser, bare til i mottakerens generelle selvbestemmelsesrett (samtykke / reservasjon) eller om det foreligger en eksisterende relasjon mellom avsender og mottaker.

Utkastet § 14 foreslås ikke å dekke markedsføringshenvendelser som skjer ved automatisert oppringningssystem. Denne metoden benyttes særlig i forbindelse med markedsføring og salg i næringsvirksomhet og av ideelle organisasjoner og en regulering reiser egne særlige spørsmål som det ikke er naturlig å regulere i utkastet § 14. Det vises blant annet til at belastningen i nettet og faren for spredning av skadelig dataprogram m.v. ikke gjør seg gjeldende på samme måte for denne metoden. Denne delen av markedsføringsloven § 2 b foreslås derfor beholdt i markedsføringsloven.

Videre bemerker utvalget at dersom overtredelsesgebyr blir tatt inn som reaksjonsform i markedsføringsloven, jf. BLDs forslag i høringsutkastet til ny markedsføringslov, bør det av praktiske årsaker vurderes en deling av spambestemmelsen mellom markedsføringsloven og straffeloven, slik at mindre spamovertredelser overfor forbruker kan følges opp av forbrukermyndighetene gjennom ileggelse av overtredelsesgebyr.

Videre vil et forbud i straffeloven effektivisere håndhevelsen, fordi straffelovens vide jurisdiksjonsbestemmelser dermed kommer til anvendelse. Dette er ikke tilfelle for et forbud som står i markedsføringsloven, som ikke rammer masseutsendelse som skjer fra utlandet. Det vises til et slikt tilfelle behandlet i Stavanger tingrettsdom av 6. oktober 2006. Etter utkastet § 14, jf. ny straffelov § 7, omfattes også utenlandske avsendere når meldingene sendes til mottakere i Norge.

### 5.6.7 Identitetstyveri

*Problemstilling*

Utvalget foreslår et eget straffebud som rammer rettsstridig bruk av uriktig identitet. I kapittel 3.5.12 er flere varianter av identitetstyveri behandlet. Problemstillingen i det følgende gjelder kun identitetstyveri ved elektronisk kommunikasjon. Et slikt straffebud antas å kunne fremme tilliten til nettbasert samhandling og være egnet til å styrke personvernet ved at den rammer krenkelser av den personlige integritet.

Ved elektronisk kommunikasjon er det enkelt å benytte uriktig identitet, men ikke alle tilfeller er kritikk- eller straffverdige. I visse sammenhenger er det kutyme for å benytte pseudonymer. Pseudonymer anses som et vidt begrep som omfatter både

navn som ikke er ens eget, men som kan fremstå som et naturlig navn, og kallenavn («nickname»/ «nick»), det vil si navn eller betegnelser som er åpenbart fiktive (for eksempel «julenissen» eller «Dolly Duck»).

Bruk av pseudonymer er for eksempel vanlig ved kommunikasjon på pratekanaler. For de øvrige parter i kommunikasjonen vil det normalt være åpenbart når det er kutyme for bruk av pseudonym og i slik sammenheng har gjerne heller ikke identiteten til avsender noen betydning for adressatene. Det kan være tvilsomt om man overhodet kan omtale slike pseudonymer som *identiteter* i forbindelse med elektronisk kommunikasjon. I hvert fall er ikke slik bruk rettsstridig. Det er heller ikke hensikten å ramme slik opptreden som er anbefalt, jf. regler om nettvett for barn og ungdom. Redd Barnas nettvettregler anbefaler barn og ungdom å unngå å oppgi sin egen identitet, og den de oppgir må derfor nødvendigvis ha karakter av å være et psudonym eller uriktig identitet. Opptreden i samsvar med slike normer, som tar sikte på å verne en brukergruppe som er spesielt utsatt, blant annet med tanke på seksuell tilnærming som «grooming», er det ikke på tale å kriminalisere gjennom en regel om identitetstyveri. Det vises også til kapitlet om nettvett i 5.3.5. Det forutsettes imidlertid at det ikke tas i bruk identitet som tilhører en annen. Slik bruk er regulært straffverdig, se nedenfor.

Det problem som et straffebud mot identitetstyveri bør rette seg mot lar seg inndele i to kategorier, henholdsvis bruk av *stjålet identitet* og *fiktiv identitet*.

Med bruk av *stjålet identitet* menes misbruk av en annens identitet. I slike tilfeller er det særlig hensynet til den hvis identitet er blitt misbrukt som begrunner et straffebud, det vil si hensynet til den personlige integritet, men handlingen kan jo også medføre en villfarelse hos den annen part i kommunikasjonen.

Med bruk av *fiktiv identitet* menes bruk av identitet som ikke er ens egen, men som heller ikke tilhører noen annen. I dette tilfellet oppstår det ikke noen identitetskrenkelse overfor noe subjekt, men det kan selvsagt oppstå en villfarelse hos den annen part i kommunikasjonen.

Det går neppe noen skarp grense mellom de to kategoriene, noe som illustreres ved bruk av identitet som er helt uriktig, men som er forvekselbar med en reell identitet. Typetilfellene er imidlertid klare og den nærmere grensedragningen må trekkes opp i rettspraksis. Siden alternativene foreslås å være er likestilte har ikke grensedragningen noen betydning for skyldspørsmålet.

*Motiv for bruk av uriktig identitet*

Det kan foreligge varierende motiv for å kommunisere under uriktig identitet. Motivet kan for eksempel være å krenke en person ved å tillegge vedkommende en mening hun ikke har. Skadeformålet kan oppnås ved å fremsette en opplysning som om den var den krenkedes egen mening, for eksempel ved å lage en uriktig erklæring i en annens navn om å begå selvmord, om avsløring av overgrep i familien eller om at man er rasist. Slike identitetstyverier kan også ramme juridiske personer, for eksempel et selskap, ved at det sendes et uriktig resultatvarsel i dets navn, eller staten, ved at det sendes en opplysning i statsministerens navn om at vedkommende stiller kabinettspørsmål, eller at statsbudsjettet sendes i navnet til finansministeren til en avisredaksjon en uke før det skal offentliggjøres.

Her er ikke poenget om opplysningene isolert sett er riktige eller uriktige, men at de er fremsatt under stjålet identitet. Det gjør handlingen ekstra graverende. I slike tilfeller er det ikke formålstjenlig å benytte fiktiv identitet, fordi ytringen da ikke smitter over på den som skal rammes.

Motivet kan også være å oppnå anonymitet for egne handlinger. For dette formålet kan man benytte både stjålet og fiktiv identitet. I tillegg kan man benytte seg av offentlig tilgjengelige anonymiseringstjenester på internett, såkalte *anonymizere*. Bruk av anonymiseringstjenester fjerner avsenderopplysningene som erstattes av anonymiseringstjenestens egne. Dette gir en form for «ikke-identitet» og er ikke i seg selv villedende for mottakeren. Men bruk av anonymiseringstjenester hindrer selvsagt muligheten for å avdekke avsenders reelle identitet, noe som er en nyttig effekt når man begår straffbare handlinger. Utvalget anbefaler derfor at myndighetene vurderer lovligheten av å tilby anonymiseringstjenester. En slik vurdering antas å burde foretas i forbindelse med en gjennomgang av straffeprosessuelle problemstillinger og spørsmålet om pliktig datalagring, jf. direktiv 2006/24/EF av 15. mars 2006. Så lenge anonymiseringstjenester ikke er ulovlige kan det heller ikke være aktuelt å kriminalisere bruken av dem, så dette faller utenfor området for utkastet § 15.

Dersom anonymitet søkes oppnådd ved å misbruke en annens eller ta en fiktiv identitet, er man innenfor det området som utvalget foreslår straffbelagt. I det første tilfellet leder handlemåten til at en annen må stå til rette for det gjerningspersonen selv har gjort. I det andre tilfellet går selve handlemåten ut over den tillit man kan ha til elektronisk kommunikasjon, og svekker datasystemenes pålitelighet.

*Om forslag til straffebud, jf. utkastet § 15*

Straffebudet tar altså sikte på å kriminalisere uberettiget bruk av uriktig identitet ved elektronisk kommunikasjon. Ovenfor er det gitt enkelte eksempler på hva som menes med uriktig identitet. Generelt gjelder det at enhver opplysning som er ment å identifisere den som står bak meldingen omfattes av straffebudets identitetsbegrep. Hva slags informasjon som er relevant i forhold til identitetsbegrepet må bero på en totalvurdering hvor konteksten tillegges stor betydning. Men opplysninger som ofte er relevante er adresseinformasjon, som for eksempel e-postadresse og webadresse (URL). I tillegg vil direkte angivelse av identitetsopplysninger som navn og adresse som oppgis på et nettsted, i en e-post eller på en pratekanal omfattes. Også innholdet på en nettside kan være opplysning om identitet og kan være rettsstridig. Det tenkes for eksempel på nettsider som har et visuelt uttrykk som er forvekselbart med nettsiden til en bedrift eller lignende. Slike nettsider anvendes ofte i forbindelse med bedragerivirksomhet som phishing, hvor de som besøker nettsiden forledes til å gi fra seg kredittkortopplysninger med videre til det som uriktig fremstår som deres egen bank.

Identiteten er uriktig når den enten tilhører en annen enn den som benytter den eller ikke tilhører noen i det hele tatt, men presenteres som om den er reell. Identiteten kan tilhøre – eller foregi at den tilhører – både et menneske og en juridisk person. Det er de samme hensyn som taler for straff i begge tilfeller.

Straffebudet gjør seg gjeldende for enhver type elektronisk kommunikasjon. Det kan skilles mellom meldinger som mottas fordi man er oppført som adressat for meldingen og informasjon på tjenester man selv oppsøker.

Dersom avsenderidentiteten er uriktig på en melding som er sendt, kommer straffebudet til anvendelse. Det kan for eksempel være tale om e-post og tekstmeldinger (sms). Såkalt phishing som utføres ved forsendelse av e-post, hvor mottaker anmodes om å avgi kontoopplysninger til en avsender som foregir å være en bankkontakt, er et praktisk tilfelle som rammes av bestemmelsen.

Identitetsopplysningene kan også være uriktige på tjenester som man selv oppsøker, for eksempel nettsider (web) på internett som uriktig opplyser å være et spesielt foretak, for eksempel en bank. Også slike nettsider anvendes ofte i forbindelse med phishing, jf. beskrivelsen ovenfor. Også tjenester man selv oppsøker er elektronisk kommunikasjon.

*Rettsstridsreservasjonen*

Bruk av uriktig identitet er bare straffbar dersom bruken er uberettiget. Det vil ha stor betydning for rettsstridsvurderingen om identiteten tillegges noen betydning i den aktuelle kommunikasjon. Det betyr at konteksten har betydning. Videre må det tas hensyn til allment anerkjente regler om nettvett. Det vises til bemerkningene innledningsvis om dette.

Forvekselbare identiteter reiser noen egne spørsmål. I en sak fra Rt. 2003 side 825 benyttet gjerningspersonene et domene som ble forvekslet med Kværner ASAs internettdomene. På grunn av forvekslingen ble Kværners identitet krenket. Gjerningspersonene hadde benyttet et domene som de selv hadde registrert, men det lå meget nær opp til Kværners eget domene (kvearner.com vs. kvaerner.com). I et slikt tilfelle kan det være en smakssak om man vil tale om en stjålet identitet eller en fiktiv identitet. Det er på det rene at man i phishing ofte benytter forvekselbare identiteter, og lykkes med det. Hvorvidt bruken er rettsstridig må vurderes konkret. Utvalget antar at spørsmålet om det foreligger en overtredelse av regler for domeneregistrering ikke bør være avgjørende. Rettsstridsvurderingen må her som ellers baseres på en totalvurdering av situasjonen. I phishingtilfellet legges det for eksempel vesentlig vekt på innholdet til nettstedet, og eventuelt innholdet i e-posten, for å bedømme om dette ligner på informasjonen til en som det ønskes å oppnå forveksling med. Da er rettsstriden på det rene, selv om det konkrete domenet kanskje ikke ville blitt bedømt som forvekselbart isolert sett.

## 5.7 Ulovlig befatning med tilgangskoder, skadelig dataprogram og utstyr, jf. utkastet §§ 10-12

### 5.7.1 Innledning

Med en fellesbetegnelse kan utkastet §§ 10, 11 og til dels § 12 sies å omhandle straffansvar for såkalte «innledende handlinger». Det vises til utdypingen av problemstillingen omkring innledende handlinger i kapittel 5.7.3.

Utvalget foreslår straffebud som rammer rettsstridig befatning med tilgangsdata, skadelig dataprogram og utstyr, jf. utkastet §§ 10-12. Straffebudene er kalt «Ulovlig befatning med tilgangsdata» (utkastet § 10), «Skadelig dataprogram og utstyr» (utkastet § 11) og «Selvspredende dataprogram» (utkastet § 12). Selvspredende dataprogram er en spesiell type skadelig dataprogram hvor den selv-

spredende egenskapen er avgjørende for om dataprogrammet omfattes av straffebudet. Hva som ellers er formålet med dataprogrammet har ikke betydning for om det omfattes av utkastet § 12.

Også andre dataprogrammer enn de selvspredende kan ha egenskaper som medfører at de kan kalles skadelige. Eksempler er dataprogram som benyttes for å trenge seg inn i datasystemer og programmer med egenskaper som «logisk bombe» som kan forårsake skade på datasystemet. Utkastet § 11 rammer spredning og andre befatningsformer med slike dataprogrammer og utstyr, mens selve bruken straffes etter de andre bestemmelsene som straffebudet viser til.

Utvalget har delt seg i spørsmålet om å innføre et straffebud som nevnt i utkastet § 11, jf. drøftelsen i kapittel 5.7.5 hvor flertallets og mindretallets syn fremgår. Flertallet går inn for å foreslå et slikt straffebud.

Dersom skadelige dataprogram har selvspredende funksjonalitet omfattes de uansett av utkastet § 12, som utvalget enstemmig stiller seg bak.

Utvalget er også enstemmig i forslaget om straff for rettsstridig befatning med tilgangskoder, jf. utkastet § 10.

### 5.7.2 Gjeldende rett

*Innledning*

Utkastet §§ 10 og 11 går inn på området for straffeloven § 145b, § 262 første ledd og åndsverkloven §§ 53a og 53c. Disse bestemmelsene omfattes av harmoniseringsforslaget. Først gis en beskrivelse av de nevnte bestemmelser. Deretter gjennomgås utvalgets tilnærming til de spørsmål som regulering av dette feltet reiser.

*Straffeloven § 145b*

Straffeloven inneholder en spesialregel om forbud mot spredning av tilgangsdata, jf. straffeloven § 145b første ledd. Selve spredningsforbudet står i første ledd som lyder:

> «Den som uberettiget gjør tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler.»

Etter annet ledd øker strafferammen til fengsel inntil 2 år dersom handlingen er grov. Blant de omstendigheter som kan tilsi at handlingen er grov nevnes om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade.

Av ordlyden fremgår det at spredningsforbudet bare gjelder tilgangsdata som kan gi tilgang til et «datasystem». Dette begrepet er ikke definert i straffeloven og benyttes heller ikke i den beslektede bestemmelsen i straffeloven § 145 annet ledd, som retter seg mot uberettiget tilgang til «data eller programutrustning». I Ot.prp. nr. 40 (2004-2005) kapittel 7.1 side 33 står det om forståelsen av § 145b at

> «uttrykket [passord eller andre data som kan gi tilgang til et datasystem] er funksjonelt avgrenset og omfatter alle data som kan gi tilgang til ulike fysiske eller logiske nivåer i et datasystem.»

Noen helt klar avgrensning av straffebudets rekkevidde gir ikke dette, men det synes naturlig at det i hvert fall skal ha samme rekkevidde som straffeloven § 145 annet ledd. Tilgangsdata som benyttes på datastyrte låssystemer på bygninger og biler m.v., faller derfor utenfor området for straffeloven § 145b.

*Straffeloven § 262 og åndsverkloven § 53a og § 53c*

Straffeloven § 262 første, jf. tredje ledd og åndsverkloven § 53a annet ledd, jf. § 54 første ledd bokstav b, gir hjemmel for straff for den som sprer eller har annen befatning med utstyr som kan bryte eller omgå elektroniske sperrer satt til vern av såkalte *vernede tjenester* og digitaliserte *vernede verk*. Selve den handling som går ut på å bryte eller omgå den elektroniske sperren er også straffbar, jf. straffeloven § 262 annet ledd og åndsverkloven § 53a første ledd. Heretter kalles den handling som bryter eller omgår sperren for «dekoding».

For oversiktens skyld gjengis de to nevnte bestemmelsene i sin helhet:

Straffeloven § 262 lyder:

> «Den som
> a) i vinnings hensikt framstiller, innfører, distribuerer, selger, leier ut, besitter, installerer, vedlikeholder eller skifter ut dekodingsinnretning,
> b) i vinnings hensikt annonserer eller på annen måte reklamerer for dekodingsinnretning, eller
> c) søker å utbre dekodingsinnretning
> når hensikten er å skaffe noen uautorisert tilgang til en vernet tjeneste, eller medvirker til dette, straffes med bøter eller fengsel inntil 1 år.
>
> Den som ved bruk av dekodingsinnretning påfører den berettigede et tap eller skaffer seg selv eller andre en vinning ved å få uautorisert tilgang til en vernet tjeneste, straffes med bøter eller fengsel inntil 6 måneder.

Med dekodingsinnretning menes i denne paragraf ethvert hjelpemiddel, enten dette er teknisk utstyr eller programvare, som er utformet eller tilpasset, alene eller sammen med andre hjelpemidler, for å gi tilgang i forståelig form til en vernet tjeneste.

Med vernet tjeneste menes i denne paragraf

a) fjernsyns- og radiosignaler, og
b) tjenester som teleformidles elektronisk på forespørsel fra den enkelte tjenestemottaker, når tilgang i forståelig form er avhengig av tillatelse fra tjenesteytere og ytes mot betaling, eller selve tilgangskontrollen til tjenestene nevnt i a og b, når den må regnes som en egen tjeneste.

Offentlig påtale finner ikke sted uten fornærmedes begjæring med mindre allmenne hensyn krever påtale. Som fornærmet regnes også den som yter tilgangskontroll når denne må regnes som en egen tjeneste.»

Åndsverkloven § 53a lyder:

«Det er forbudt å omgå effektive tekniske beskyttelsessystemer som rettighetshaver eller den han har gitt samtykke benytter for å kontrollere eksemplarfremstilling eller tilgjengeliggjøring for allmennheten av et vernet verk.

Det er videre forbudt å:

a) selge, leie ut eller på annen måte distribuere,
b) produsere eller innføre for distribusjon til allmennheten,
c) reklamere for salg eller utleie av,
d) besitte for ervervsmessige formål, eller
e) tilby tjenester i tilknytning til innretninger, produkter eller komponenter som frembys med det formål å omgå effektive tekniske beskyttelsessystemer, eller som kun har begrenset ervervsmessig nytte for annet enn slikt formål, eller som i hovedsak er utviklet for å muliggjøre eller forenkle slik omgåelse.

Bestemmelsen i denne paragraf skal ikke være til hinder for forskning i kryptologi. Bestemmelsen i første ledd skal heller ikke være til hinder for privat brukers tilegnelse av lovlig anskaffet verk på det som i alminnelighet oppfattes som relevant avspillingsutstyr. For tekniske innretninger til beskyttelse av et datamaskinprogram gjelder i stedet det som er bestemt i §53c.

Bestemmelsene i første ledd skal ikke være til hinder for eksemplarfremstilling etter §16.»

Hva som er *vernede tjenester* er nærmere angitt i straffeloven § 262 fjerde ledd og omfatter betalingsbelagte tilgangskontrollerte kringkastingssignaler og informasjonssamfunnstjenester. I tillegg omfattes tilgangskontrollen som sådan når den må regnes som en vernet tjeneste. Det kan nemlig tenkes at det er forskjellige rettighetshavere til innholdet og distribusjonssystemet, og til den teknologien som beskytter tilgangen til innholdet. Et eksempel er beskyttelsessystemet Content Scrambling System som ble anvendt på dvd-filmer. Dette systemet ble lisensiert separat til produsenter av dvd-spillere og innholdsleverandørene, se faktabeskrivelsen i dvd-dommen i RG 2004 side 414.

Det strafferettslige vernet mot uberettiget dekoding av beskyttede kringkastingssignaler ble innført i straffeloven § 262 ved lov av 7. april 1995 nr. 15. Ved endringsloven av 15. juni 2001 nr. 57, ble vernet utvidet til å omfatte betalingsbelagte tilgangskontrollerte informasjonssamfunnstjenester og tilgangskontrollen som sådan når den må regnes som en egen tjeneste. Ved denne lovendringen ble også det strafferettslige forsøks- og medvirkningsansvaret mer detaljert utpenslet slik det fremgår av første ledd.

Åndsverkloven § 53a er utformet på lignende måte som straffeloven § 262, og retter seg mot uberettiget dekoding av digitaliserte åndsverk (vernede verk) og nærmere angitte forberedelses- og medvirkningshandlinger til slik dekoding. Hva som er å anse som åndsverk fremgår av åndsverkloven § 1. Verkene nevnt i denne bestemmelsen kan være representert i forskjellig form, og det er bare når de er representert digitalt at de kan være tilgangskontrollert og beskyttet mot uberettiget dekoding, jf. åndsverkloven § 53a. Film og musikk har lenge vært distribuert til markedet i digitalisert form. For å sikre kontroll mot uberettiget spredning benyttes tilgangskontroll på samme vis som for de vernede tjenester nevnt ovenfor. Dataprogrammer er åndsverk som er representert digitalt og er omfattet av det generelle dekodingsvernet etter ordlyden i åndsverkloven § 53a første ledd. Av bestemmelsens tredje ledd siste punktum fremgår det imidlertid at vernet mot uberettiget dekoding skal følge åndsverkloven § 53c, som følgelig er en spesialregel for dataprogrammer. Åndsverkloven § 53c lyder:

«Omsetning av, eller besittelse i ervervsøyemed av et hvilket som helst middel hvis eneste formål er å gjøre det lettere ulovlig å fjerne eller omgå tekniske innretninger til beskyttelse av et datamaskinprogram, er forbudt.»

Denne bestemmelsen har sin forankring i programvaredirektivet 1991/250/EØF av 14. mai 1991, og er beslektet med åndsverkloven § 53a annet ledd, se under kapitlet «Åndsverkloven § 53c» nedenfor.

Hovedregelen om eneretten er angitt i åndsverkloven § 2 første ledd som lyder:

> «Opphavsretten gir innen de grenser som er angitt i denne lov, enerett til å råde over åndsverket ved å fremstille varig eller midlertidig eksemplar av det og ved å gjøre det tilgjengelig for almenheten, i opprinnelig eller endret skikkelse, i oversettelse eller bearbeidelse, i annen litteratur- eller kunstart eller i annen teknikk.»

Eneretten gjelder altså eksemplarfremstilling (kopiering) og tilgjengeliggjøring for allmennheten. Som følge av at elektronisk overføring av verk på individuell basis er blitt en vanlig kommersiell spredningsform, ble tilgjengeliggjøringsalternativet presisert ved lovendring 17. juni 2005 nr. 97, for å sikre at også slik distribusjon omfattes av eneretten. Presiseringen er inntatt i åndsverkloven § 2 tredje ledd bokstav c, jf. fjerde ledd, og lyder:

> «Verket gjøres tilgjengelig for allmennheten når
> c) verket fremføres offentlig.
> Som offentlig fremføring regnes også kringkasting eller annen overføring i tråd eller trådløst til allmennheten, herunder når verket stilles til rådighet på en slik måte at den enkelte selv kan velge tid og sted for tilgang til verket.»

Bestemmelsen gjelder også for plate- og filmprodusenters rettigheter, jf. henvisningen i åndsverkloven § 45 siste ledd. Når slike distribusjonstjenester er tilgangskontrollert, er de vernet mot uberettiget dekoding, jf. åndsverkloven § 53a.

### *Sammenhengen mellom straffeloven §§ 145b, 262 og åndsverkloven § 53a*

Det er et tydelig slektskap mellom straffeloven § 262 og åndsverkloven § 53a både hva gjelder den type innhold som er beskyttet og de beskyttelsesteknikker som forutsettes anvendt og som nyter strafferettslig beskyttelse. De vernede tjenester etter straffeloven § 262 vil jevnlig bestå i opphavsrettslig vernet materiale som også er vernet etter reglene i åndsverkloven. Men straffeloven § 262 rekker videre siden den omfatter enhver type innhold bare det er distribuert slik bestemmelsen angir. Det vil si at den omfatter vernede verk etter åndsverkloven, men ikke er begrenset til dette.

Åndsverkloven § 53a går lenger enn straffeloven § 262 i ett henseende. Bestemmelsen oppstiller nemlig også vern for tilgangskontrollerte *eksemplarer* av verk. I praksis er dette cd-er og dvd-er med musikk og film. Slike eksemplarer faller utenfor området for straffeloven § 262, se bestemmelsens fjerde ledd, som forutsetter at det skjer en elektronisk overføring fra tjenesteyter til tjenestemottaker. Også før innføringen av åndsverkloven § 53a har slike eksemplarer av digitaliserte åndsverk hatt et visst vern mot uberettiget dekoding, jf. straffeloven § 145 annet ledd. I hvert fall ble dette syn lagt til grunn av Borgarting lagmannsrett i dvddommen (RG 2004 side 414). En annen sak er at lagmannsretten kom frem til at dekodingen i det nevnte tilfellet ikke var uberettiget. Etter innføringen av åndsverkloven § 53a er det rimelig å anta at denne gjelder som *lex specialis* for slike tilfeller.

Dataprogrammer reiser noen egne spørsmål som behandles i neste underkapittel.

Straffeloven § 145b har sin bakgrunn i datakrimkonvensjonen artikkel 6. Konvensjonsbestemmelsen pålegger medlemmene på visse betingelser å kriminalisere besittelse, produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte av skadelig programvare og tilgangskoder som gir tilgang til hele eller deler av et datasystem. Bestemmelsen legger altså opp til at partene til konvensjonen innfører straffebud som rammer nærmere angitte forberedelses- og medvirkningshandlinger til krenkelser av data og datasystemer.

Artikkel 6 er bygget opp over samme lest som de konvensjonsbestemmelser som ligger til grunn for utformingen av straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd. Det vises til tilgangskontrollkonvensjonen artikkel 4, tilgangskontrolldirektivet artikkel 4 og opphavsrettsdirektivet artikkel 6. Lovgiver har gjennomført de nevnte bestemmelser fullt ut redaksjonelt og innholdsmessig i straffeloven § 262 og åndsverkloven § 53a.

Ved gjennomføringen av artikkel 6 i den interne rett ved lovendringen av 8. april 2005 nr. 16, benyttet lovgiver reservasjonsadgangen i artikkel 6 nr. 3, jf. artikkel 40, og innførte et straffebud i straffeloven § 145b som var begrenset til å oppfylle minimumsforpliktelsen. Denne gjaldt spredning av tilgangskoder som kan gi tilgang til hele eller deler av et datasystem. Selve den uberettigete tilgang til datasystemet rammes av straffeloven § 145 annet ledd. Det systematiske forhold mellom disse to straffebestemmelsene tilsvarer forholdet mellom første og tredje ledd i straffeloven § 262, og første og annet ledd i åndsverkloven § 53a.

De dekodingsinnretninger som er nevnt i straffeloven § 262 tredje ledd og åndsverkloven § 53a, omfatter både dataprogrammer, fysisk utstyr og tilgangskoder. Det vises til Ot.prp. nr. 51 (2000-2001) kapittel 6.4, hvor Justisdepartementet skriver at

> «Omgrepet skal dekke alle hjelpemiddel, anten dette er utstyr (hardware) eller programvare

> (software), som er utforma eller tilpassa – åleine eller saman med andre hjelpemiddel – for å gi tilgang i forståeleg form til ei verna teneste. [...] Kodar, kodenøklar og passord vil normalt vere innretningar som har dei egenskapane som etter definisjonen konstituerer ei dekodarinnretning.»

Det vises også til Ot.prp. nr. 46 (2004-2005) side 119 flg., hvor det på side 120 i kapittel 3.5.1.5.4 står at

> «Med omgåelsesverktøy menes innretning, produkt, komponent eller tjeneste som tilbys eller ytes i forbindelse med omgåelse av tekniske beskyttelsessystemer.»

Tilgangskoder er en vanlig bestanddel i slike beskyttelsesinnretninger og det anses ikke som tvilsomt at tilgangskoder omfattes av alternativet «komponenter» i åndsverkloven § 53a annet ledd. Problemstillingen er ekvivalent med det som gjelder for dekodingsinnretning, jf. straffeloven § 262 tredje ledd.

Tilgangskoder kan være integrert i dataprogrammer og utstyr som anvendes for dekoding. Det vil for eksempel være tilfelle når et smartkort er kodet med en tilgangskode til en betalingsbelagt fjernsynssending, eller når et dataprogram som fjerner beskyttelsen på dvd-filmer inneholder tilgangsdata som «åpner» filmen. Men tilgangsdata kan også fungere alene. For eksempel gjelder det tilgangsdata som benyttes for å logge inn på en brukerkonto på et datasystem, en pinkode til bruk på minibank eller en tilgangskode til en internettjeneste, for eksempel en som tilbyr filmfremvisning. Uberettiget anskaffelse, markedsføring og spredning m.v. av tilgangskoder er straffbart etter straffeloven § 262 og åndsverkloven § 53a uavhengig av om befatningen gjelder tilgangskoden alene, eller om den er integrert i fysisk utstyr eller programvare. I begge tilfeller er tilgangskoden en dekodingsinnretning,

Rekkevidden av straffeloven § 145b er noe mer uklar. Forarbeidene synes å forutsette at tilgangskodene spres uten at de er integrert i fysisk utstyr eller programvare. De spres for eksempel via nettsteder på internett. Slike tilfeller av rettsstridig spredning er straffbar etter straffeloven § 145b. Dersom tilgangskodene er integrert i smartkort og spres som følge av at selve smartkortet uberettiget omsettes, er det uklart om § 145b kommer til anvendelse.

### *Åndsverkloven § 53c*

Dataprogrammer står i en særstilling i forhold til de regler som er behandlet i det foregående. På samme vis som musikk og film distribueres dataprogrammer som eksemplarer på cd og ved elektronisk overføring, for eksempel fra en tjenesteyter på internett. Rent teknisk forsøkes disse distribusjonsformene for dataprogrammer sikret ved bruk av tilgangskontroll på samme måte som for film og musikk.

Omsetning eller besittelse i ervervsøyemed av dekodingsutstyr som kan anvendes til å foreta uberettiget dekoding av tilgangskontroll på dataprogram er forbudt og straffbart, jf. åndsverkloven § 53a, jf. § 54 første ledd bokstav b. Det vises til sitatet av § 53c ovenfor. Denne regelen er som nevnt beslektet med åndsverkloven § 53a annet ledd. Av § 53c tredje ledd siste punktum, følger det at «For tekniske innretninger til beskyttelse av et datamaskinprogram gjelder i stedet det som er bestemt i § 53c».

Spørsmålet gjelder fortolkningen av «i stedet» i § 53a tredje ledd tredje punktum. Henviser formuleringen til hele § 53a eller bare til den delen av bestemmelsen som korresponderer med § 53c, nemlig annet ledd i § 53a? Hvis det første alternativet skal legges til grunn er rettstilstanden at de innledende handlinger rammes av § 53c, mens dekodingen rammes av § 53a første ledd. Det betyr at dataprogram likebehandles med andre digitaliserte åndsverk for så vidt gjelder dekodingen. Ordlyden i § 53a første ledd gir anvisning på denne løsningen, siden den setter forbud mot omgåelseshandlinger for vernede verk generelt, noe som også omfatter dataprogram, jf. åndsverkloven § 1 annet ledd nr. 12. Setningen i § 53a tredje ledd siste punktum fremstår som løsrevet fra de to foregående, hvorav første punktum henviser til hele § 53a, jf. «denne paragraf», mens annet punktum bare viser til «første ledd». Etter struktur og ordlyd i selve § 53a er det dermed intet til hinder for å legge ovenstående fortolkning til grunn.

Forarbeidene til § 53a tredje ledd tredje punktum og § 53c taler imidlertid imot at dataprogram har vern mot uberettiget dekoding, jf. § 53a første ledd. Det vises til uttalelsene i Ot.prp.nr 46 (2004-2005) på side 122-123 og 157, hvor det fremgår at omgåelsesforbudet i sin helhet reguleres i § 53c. Resultatet henger dårlig sammen med det strenge vern som for øvrig er gitt dataprogrammer, jf. forbudet mot privatkopiering, utlån og analyse / omvendt utvikling, jf. åndsverkloven §§ 12 annet ledd bokstav b, § 19 annet ledd, § 39h og § 38i.

Det fremgår av forarbeidene at det som ble gjort var å flytte det eksisterende forbudet i åndsverkloven § 54a til § 53c. Forarbeidene ses ikke å inneholde noen vurdering av hvordan omgåelseshandlingene som sådan skal reguleres. Det er derfor grunn til å reise spørsmål om man utilsiktet har

unnlatt å skaffe hjemmel for å forby og straffe slik omgåelse overfor tilgangskontroll av dataprogram, eller om meningen nettopp har vært at handlingen omfattes av § 53a første ledd, slik at formuleringene i forarbeidene er noe ufullstendige på dette punkt.

Omgåelseshandlinger overfor dataprogrammer kan uansett anses som en del av harmoniseringsspørsmålet som for fremtiden bør reguleres og ha et vern på linje med andre data. Lovforslaget legger opp til dette.

Siden det vesentlige av tematikken i kapitlet 5.7 gjelder kriminalisering av innledende handlinger, berører samordningsspørsmålet for dataprogrammer særlig den gjeldende bestemmelse i åndsverkloven § 53c. Selve omgåelsen av tilgangskontroll på dataprogrammer rammes av de regler i lovforslaget som gjelder uberettiget tilgang, informasjons- og datatyveri, jf. utkastet §§ 4-6, som er behandlet i kapittel 5.5.2 og 5.6.2. Det vises også til merknadene i kapittel 5.3 om rettsstridsreservasjonen.

### 5.7.3 Utvalgets tilnærming

*Fremskutt innslagspunkt for straff*

Begrunnelsen for kriminalisering av befatning med tilgangskoder og skadelig programvare, er først og fremst at slike handlinger kan være – og ofte vil være – første skritt for å muliggjøre ulovlig inntrengning i datasystem eller for å foreta datamodifikasjon. På denne måten vil befatning med tilgangskoder og skadelig programvare kunne sies å være innledende handlinger til andre straffbare handlinger. Man kan dermed si at kriminalisering av slike handlinger først og fremst er et spørsmål om straffelovens innslagspunkt, det vil si om man skal anvende et såkalt fremskutt innslagspunkt for straff. Reglene suppleres av det alminnelige strafferettslige forsøks- og medvirkningsansvaret, jf. ny straffelov §§ 15 og 16.

Det kan nevnes at spredningsalternativet i utkastet § 12 er beslektet med utkastet § 7, fordi spredningen av selvspredende dataprogram kan anses som en spesiell form for dataskadeverk. En slik handling leder med nødvendighet til endringer på de datasystemer som infiseres av programmet.

Selve *bruken* av tilgangsdata og skadelig programvare rammes som nevnt av andre straffebud i lovforslaget, forutsatt at bruken er rettsstridig. Dette gjelder for eksempel bruk av et stjålet passord for å skaffe seg uberettiget tilgang til et datasystem, jf. utkastet § 4 og aktivisering av et dertil egnet dataprogram som skaper driftshindring, jf. utkastet § 13. Befatning med et stjålet passord kan også være straffbar som informasjonsheleri, jf. utkastet § 9 og straffeloven § 317.

Det kan være grunn til å understreke at ulovlig dekoding som sådan, jf. straffeloven §§ 145 annet ledd (når overtredelsen skjer ved beskyttelsesbrudd), 262 annet ledd og åndsverkloven § 53a første ledd, jf. § 54, dekkes av utkastet §§ 4-6. Disse straffebudene i lovforslaget rammer den som uberettiget skaffer seg tilgang til et datasystem, og den som uberettiget tilegner seg databasert informasjon og data. Overtredelsen kan være begått ved at det er foretatt dekoding, men dette er ikke noen betingelse for straff. Det betyr at bestemmelsene har et videre anvendelsesområde enn det som følger av de nevnte bestemmelser i straffeloven og åndsverkloven. En overtredelse som har skjedd ved dekoding kan medføre at lovbruddet skal anses å være grovt, jf. utkastet § 18. Det vises til bemerkningene i kapittel 5.5.2 og 5.6.2.

Poenget er at overtredelse for §§ 4-6 ikke er betinget av at datasystemet, den databaserte informasjonen eller dataene er tilgangskontrollert. Den legislative begrunnelse for dette er beskrevet i kapittel 5.5.1 og 5.6.1. Med andre ord er det tilstrekkelig for overtredelse at adgangen eller tilegnelsen er uberettiget. Dekoding er derfor bare én av flere mulige overtredelsesformer.

Utkastet §§ 10-12 retter seg mot det å anskaffe, fremstille, modifisere, markedsføre og tilgjengeliggjøre tilgangsdata og skadelig dataprogram (for en nærmere beskrivelse av de forskjellige alternativene vises det til spesialmotivene i kapittel 9.10-9.12). Skadelig dataprogram omfatter mer enn den type programvare og utstyr som kan anvendes for å skaffe seg uberettiget adgang til datasystemer, databasert informasjon eller data. Dette følger av henvisningen i straffebudet som omfatter §§ 4-8, 10 og 13-14. Foruten de straffebud som dekker området for straffeloven §§ 145 annet ledd, 145b, 262 og åndsverkloven 53a, jf. utkastet §§ 4-6, omfattes utkastet § 7 (datamodifikasjon), § 8 (uberettiget bruk av datasystem), § 10 (ulovlig befatning med tilgangsdata), § 13 (driftshindring) og § 14 (masseutsendelse av elektroniske meldinger).

Begrunnelsen for utkastet §§ 10-11 er at de nevnte handlinger øker faren for at den direkte krenkelse begås, typisk datainnbrudd, informasjonstyveri, datamodifikasjon, og driftshindring. For utkastet § 10 gjør det seg i tillegg gjeldende at konfidensiell behandling av tilgangsdata er en forutsetning for at den skal kunne fungere på en sikker måte. Rettsstridige krenkelser av konfidensialiteten rammes derfor av utkastet § 10. Det vises også til bemerkningene om datasikkerhet, konfidensialitet og autentisering i kapittel 4.6.2.

Alternativet «besittelse» har vært undergitt en nærmere vurdering. Utvalget har kommet frem til at det bør inntas i utkastet §§ 10 og 11, men ikke i utkastet § 12. Det vises til bemerkningene i forbindelse med de respektive straffebud.

Straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd hjemler allerede et fremskutt strafferettslig innslagspunkt for verktøy som kan anvendes til å foreta uberettiget dekoding av vernede tjenester og verk. Det samme gjelder åndsverkloven § 53c. Lovforslaget innebærer en generalisering slik at den rettsstridige befatning gjøres straffbar for tilgangsdata og verktøy som gjelder data, databasert informasjon og datasystemer uavhengig av lagrings- og distribusjonsform og innholdets karakter.

Utkastet §§ 10-11 dekker dermed området for straffeloven §§ 145b, 262 første ledd og åndsverkloven § 53a annet ledd og § 53c. Dersom lovforslaget blir gjennomført, er det ikke nødvendig å videreføre de nevnte bestemmelsene. Lovforslaget harmoniserer de nevnte bestemmelser og gjør ellers ikke noen endring i rettstilstanden.

### *Nykriminalisering*

Utkastet § 10 innebærer en viss nykriminalisering. Etter dagens regler er spredning av tilgangsdata straffbart dersom de kan gi tilgang til datasystem, vernede tjenester eller verk, jf. straffeloven §§ 145b, 262, åndsverkloven § 53a og § 53c. Foruten spredning rammer straffeloven § 262 og åndsverkloven § 53a også det å fremstille, innføre, besitte, installere, vedlikeholde, skifte ut, annonsere og markedsføre, og tilby tjenester i tilknytning til, slike dekodingsinnretninger. Forbudet etter straffeloven § 145b som gjelder tilgangskoder som kan gi tilgang til et datasystem er begrenset til å gjelde *spredning* av slike tilgangsdata.

Utvalget går enstemmig inn for at også de øvrige befatningsformer bør være straffbare for tilgangskoder som gir tilgang til datasystem generelt. Utkastet § 10 gir derfor anvisning på et mer omfattende forbud enn det som følger av straffeloven § 145b, men i lys av den vide rekkevidden av straffeloven § 262 og åndsverkloven § 53a, representerer utkastet § 10 likevel bare en mindre nykriminalisering.

Utkastet § 11 innebærer nykriminalisering av befatning med skadelig dataprogram og utstyr som rammer andre datasystemer og dataoverføringer enn de som er omfattet av straffeloven § 262, åndsverkloven § 53a og § 53c. Dette følger av at utkastet § 11 gjelder verktøy som kan ramme datasystemer generelt, ikke bare slike som omfattes de nevnte bestemmelsene. For eksempel vil anskaffelse og spredning av skadelig dataprogram som kan benyttes for å trenge inn i datasystemet til en bedrift, rammes av utkastet § 11. Det samme gjelder anskaffelse og spredning av utstyr som kan benyttes til å avlytte telefonsamtaler. Dette er ikke straffbart i dag, med mindre handlingen kan anses som medvirkning til datainntrengningen eller avlyttingen. Vilkårene for medvirkningsansvar vil etter gjeldende rett neppe være oppfylt for den som sprer skadelig dataprogram fra et nettsted, men ikke deltar i den konkrete utnyttelsen av programmet verken fysisk eller psykisk. Slik spredning foregår i stor utstrekning på internett og anses av mange som et stort problem. Utkastet § 11 rammer altså slike handlinger.

### *Redaksjonelle hensyn*

Utvalget har valgt å redigere lovforslaget slik at befatning med tilgangskoder og skadelig dataprogram reguleres i forskjellige bestemmelser. I straffeloven § 262 og åndsverkloven § 53a og § 53c er tilgangskoder og skadelig programvare behandlet under ett med felles betegnelse, jf. «dekodingsinnretning» i § 262 tredje ledd, «innretninger, produkter eller komponenter» i § 53a annet ledd og «middel» i § 53c. Alle uttrykkene omfatter både dataprogrammer, fysisk utstyr og tilgangskoder.

Utvalget mener at det er hensiktsmessig å oppstille særskilte regler for befatning med henholdsvis tilgangsdata og skadelig dataprogram m.v. Dermed får man bedre frem de rettspolitiske hensyn bak bestemmelsene.

Som nevnt vil tilgangskoder ofte være integrert i dataprogrammer og utstyr som benyttes for å foreta dekoding. Slike tilfeller rammes av utkastet § 11. Utkastet § 10 kommer til anvendelse der befatningen gjelder tilgangskodene direkte, for eksempel ved passordknekking, ved spredning av tilgangsdata på internett eller ved omsetning av en cd-rom hvor man har kopiert tilgangsdata.

Befatning med selvspredende dataprogram, jf. utkastet § 12, anses som meget skadelig i seg selv. Den legislative begrunnelse for straff står således på egne ben og det er naturlig å utforme forbudet i en egen bestemmelse. Legaldefinisjonen av selvspredende dataprogram er tatt inn i utkastet § 12 tredje ledd, siden begrepet utelukkende benyttes i denne bestemmelsen. En integrering av utkastet §§ 11 og 12 i én bestemmelse ville gjøre den så komplisert at det også av den grunn er hensiktsmessig med to bestemmelser. De rettspolitiske spørsmål bak bestemmelsene er heller ikke helt sammenfallende. Særlig kan det herske ulike syn

på hvor skadelig og straffverdig handlingene i utkastet § 11 er, og om hvor effektivt straffebudet vil være. Slike hensyn ligger til grunn for mindretallets dissens vedrørende utkastet § 11, men gjør seg altså ikke gjeldende på samme måte for utkastet § 12.

### 5.7.4 Uberettiget befatning med tilgangsdata, jf. utkastet § 10

Utkastet § 10 første ledd lyder:

> «For ulovlig befatning med tilgangsdata straffes den som uberettiget anskaffer, innfører, fremstiller, besitter, markedsfører eller gjør tilgjengelig for andre passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem.»

Det sentrale uttrykket er «tilgangsdata [...] som kan gi tilgang til data, databasert informasjon eller datasystem». Tilgangsdata er kjennetegn som for eksempel tegnstrenger (passord) eller et digitalisert fingeravtrykk. Data, databasert informasjon og datasystemer er legaldefinert i utkastet § 1. I kontekst av utkastet § 10 forutsettes det at de nevnte objekter er tilgangskontrollert slik at utnyttelsen krever bruk av tilgangsdata.

De befatningsformer som er nevnt dekker alle alternativ etter datakrimkonvensjonen artikkel 6, straffeloven §§ 145b, 262 første ledd, åndsverkloven § 53a annet ledd og § 53c.

Begrunnelsen for straffebudet er, foruten de folkerettslige forpliktelser som det tidligere er redegjort for, at en tilgangskode bare har verdi for den berettigete dersom den er hemmelig. Det er bare da den kan fungere som sikkerhet for konfidensialitet og som mekanisme for autentisering (det vil si at den kan bekrefte identiteten til brukeren, se kapittel 4.6.2 om autentisering).

Det at tilgangskoder blir kjent for andre og eventuelt spredt, har store skadevirkninger for rette innehaver av tilgangskoden og for datasystemets eier. Dermed svekkes også tilliten til datasystemene, se om hensynene til tillit og pålitelighet i kapittel 4.6.1. Dette tilsier at konfidensialitetshensynet understøttes med et straffebud som utkastet § 10.

Det ses ikke at et forbud mot befatning med tilgangskoder vil gå ut over hensynene til læring, forskning og kreativitet, jf. kapittel 4.5.4. Muligheten for å foreta analyse av dataprogram er viktig for den teknologiske utvikling og denne retten rammes ikke. Dersom man under analysen av et dataprogram kommer over tilgangsdata som er implementert i programmet, kan man tenkes å falle inn under anskaffelsesalternativet i utkastet § 10 rent objektivt, men en slik anskaffelse vil ikke være rettsstridig dersom analysen ellers skjer på lovlige vilkår, slik dette følger av reglene i åndsverkloven §§ 39h og 39i. Imidlertid kan den fortsatte besittelse av tilgangsdataene være straffbar, jf. besittelsesalternativet i utkastet § 10. Det samme gjelder en eventuell spredning av tilgangsdataene. Poenget er at retten til å analysere dataprogram er begrunnet i ønsket om å tilrettelegge for at man kan sette seg inn i de ideer og prinsipper som programmet er bygget på.

Det kan vises til fortalen i programvaredirektivet hvor det blant annet står:

> «For at det ikke skal oppstå tvil må det presiseres at det bare er et datamaskinprograms uttrykksform som er beskyttet, og at de ideer og prinsipper som ligger til grunn for de enkelte delene av programmet, herunder de som ligger til grunn for programmets grensesnitt, ikke er opphavsrettslig beskyttet etter dette direktiv.
>
> I samsvar med dette prinsippet om opphavsrett og i den utstrekning logikk, algoritmer og programmeringsspråk utgjør ideer og prinsipper, er ikke disse ideene og prinsippene beskyttet i henhold til dette direktiv. »

Analyseretten kan følgelig ikke gi rett til å avdekke tilgangskoder. Kodene er konkrete uttrykk og ikke ideer eller prinsipper. Dertil kommer at slike tilgangskoder er ment å være hemmelige og dette er en nødvendig egenskap for at de skal fungere effektivt. Man kan derfor ikke skyte seg inn bak analyseretten dersom hensikten først og fremst er å avdekke tilgangskodene.

Dette skillet mellom vernet om ideer og prinsipper og vernet om tilgangskoder antas å være i samsvar med *Kerckhoffs prinsipp,* som anses å være grunnleggende innen kryptosikkerhet og teknisk analyse. Prinsippet går blant annet ut på at kryptosikkerhet ikke skal være avhengig av hemmelighold av algoritmen som et program er bygget på, men være basert på hemmelighold av tilgangskoden. Selve algoritmen skal være åpen og kunne la seg analysere, og i dette ligger et vesentlig bidrag til teknologisk utvikling. Algoritmen kan sies å være uttrykk for de ideer og prinsipper som ligger til grunn for dataprogrammet, i motsetning til tilgangskoden som altså er et konkret uttrykk som både kan og bør ha et lovfestet konfidensialitetsvern.

Avdekking av tilgangskoder som skjer som ledd i analyse av dataprogram kan være straffbar etter utkastet § 10, dersom avdekking skjer forsettlig og analysen kunne vært lagt opp slik at avdek-

king av koden kunne vært unngått. Avdekking som skjer uforsettlig vil ikke være straffbar. Derimot vil forsettlig besittelse etter at koden uforsettlig er avdekket være straffbar etter utkastet § 10. For å unngå å komme i straffansvar må man i slike tilfeller følgelig slette tilgangskoden.

Av hensyn til behovet for hemmelighold av tilgangskoder straffes også den som «fremstiller» slike koder. Tilgangskoder kan for eksempel gjettes ved maskinell passordknekking. Dette omfattes av fremstillingsalternativet. Det vises for øvrig til spesialmotivene for kommentarer til de enkelte alternativ i gjerningsbeskrivelsen, se kapittel 9.10.

### 5.7.5 Skadelig dataprogram og utstyr, jf. utkastet § 11

*Innledning*

Utkastet § 11 første ledd lyder:

> «For ulovlig befatning med skadelig dataprogram straffes den som uberettiget anskaffer, fremstiller, modifiserer, besitter, markedsfører eller tilgjengeliggjør dataprogram som er særlig egnet til å begå handlinger som er straffbare etter §§ 4-8, 10 eller 13-14 i dette kapitlet. Liknende befatning med utstyr som er særlig egnet til tilsvarende formål straffes på samme måte.»

*Historikk*

Lovgiver har tidligere valgt å avstå fra å kriminalisere befatning med skadelig dataprogram og utstyr. Datakrimutvalget drøftet problemstillingen i delutredning I (NOU 2003: 27) på side 18 flg., og konkluderte med at det ikke var tilrådelig å innføre noe slikt straffebud. Det ble vist til at de generelle regler om forsøk og medvirkning stort sett ville være tilstrekkelige. Videre ble det antatt at et slikt straffebud i stor grad måtte basere seg på vilkår av subjektiv art, det vil si gjerningspersonens hensikt med befatningen. Slik «sinnelagsstrafferett» ville bryte med norsk strafferettslig tradisjon. Utvalget hadde dessuten i utgangspunktet besluttet å fremme et minimumsforslag, det vil si bare det som var nødvendig for å ratifisere datakrimkonvensjonen. Også av denne grunn valgte man å anbefale at Norge benyttet seg av reservasjonsadgangen. Datakrimutvalget anbefalte følgelig bare å kriminalisere spredning av tilgangskoder, jf. artikkel 6 nr. 1, a, ii.

I høringsrunden gjorde det seg gjeldende svært ulike syn på behovet for et straffebud om befatning med verktøy som gir ulovlig tilgang til datasystem, jf. Ot.prp. nr. 40 (2004-2005) i kapittel 3.3.4 side 16 flg. Innvendingene var i stor grad de samme som Datakrimutvalget hadde vist til. Men særlig ØKOKRIM tok til orde for innføring av et straffebud og karakteriserte slikt verktøy som «elektronisk sprengstoff» som det var grunn til å forby. ØKOKRIM fremhevet at bruken av verktøy som gir ulovlig tilgang til datasystem

> «representerer et enormt samfunnsmessig problem, og det er derfor overraskende at Datakrimutvalget ikke har vurdert konvensjonen artikkel 6 mer grundig på dette punkt.»

Departementet fremmet et mer omfattende lovforslag enn Datakrimutvalget hadde foreslått og gikk inn for også å kriminalisere befatning med denne typen verktøy. Departementets utgangspunkt var at det krever en

> «tungtveiende begrunnelse for å sette straff for forberedelseshandlinger. I samme retning trekker ønsket om ikke å knytte grensen for det straffbare i for stor grad til rent subjektive forhold [...]. Dette synspunktet får imidlertid mer begrenset bærekraft når den aktuelle forberedelseshandlingen i større utstrekning enn helt hverdagslige handlinger bidrar til å kaste lys over gjerningspersonens forsett.»

Departementet oppsummerte sitt syn på spørsmålet slik:

> «Etter departementets syn taler både det betydelige skadepotensialet, hensynet til tilliten til elektronisk kommunikasjon som kommunikasjonsform og den tilsynelatende lave oppdagelsesrisikoen for at det bør være straffbart å besitte hackerverktøy og andre tilsvarende innretninger. En slik straffebestemmelse lar seg ikke bare forsvare ut fra de prinsippene for kriminalisering som det er redegjort for i Ot.prp. nr. 90 (2003-2004) s. 88 flg. Det vil også lette det internasjonale samarbeidet i saker som gjelder datakriminalitet, især hvor samarbeidet er betinget av at den handlingen som det er tale om, er straffbar også etter norsk rett. Departementet nevner for øvrig, uten at det har vært avgjørende, at slike handlinger allerede er straffbare etter dansk rett. [...]. Etter departementets syn har de momentene som det er vist til i drøftelsen ovenfor, minst like stor gjennomslagskraft i spredningstilfellene.»

Lovforslaget, inntatt i Ot.prp. nr. 40 (2004-2005) side 37, som ble fremmet for behandling av Stortinget, lød som følger:

> «Ny §145 b skal lyde:
> Den som uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for andre

a) passord eller andre data som kan gi tilgang til et datasystem, eller
b) dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer straffes med bøter eller fengsel inntil 6 måneder eller begge deler.

Grove overtredelser straffes med fengsel inntil 2 år. Ved avgjørelsen av om overtredelsen er grov, skal det blant annet legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen skaper fare for betydelig skade.

Medvirkning straffes på samme måte.»

Justiskomiteen i Stortinget delte seg i synet på å gjennomføre § 145b som foreslått i lovproposisjonen, se Innst. O. nr. 53 (2004-2005) kapittel 2.

Flertallet bestående av representanter fra Arbeiderpartiet, Fremskrittspartiet og Sosialistisk Venstreparti (til sammen 6 representanter) påpekte

«at problemstillingen om å kriminalisere forberedelseshandlinger har vært gjenstand for betydelig debatt. Flertallet vil således vise til et sitat fra en av våre nestorer innen strafferetten, Johs. Andenæs, som har forklart grensen mellom straffri forberedelse og straffbart forsøk på følgende måte:

«Gjerningsmannens opptreden må vise at nå er forberedelsens og overveielsens tid forbi, nå skrider han til verket».

Flertallet er på denne bakgrunn av den oppfatning at Norge bør benytte seg av den reservasjonsadgang som er oppstilt i konvensjonens artikkel 6 nr. 3. Dette innebærer at Norge ikke forplikter seg til å kriminalisere de forhold tilknyttet nevnte problemstilling som er beskrevet i konvensjonens artikkel 6, med unntak av de handlinger som fremgår av artikkel 6 nr. 1 a) ii.»

Mindretallet oppsummerte sitt syn på følgende måte:

«Komiteens medlemmer fra Høyre og Kristelig Folkeparti er enig i at det skal sterke grunner til for å kriminalisere forberedelseshandlinger, og viser til departementets drøftelse på side 17 og 18 i proposisjonen. Disse medlemmer mener likevel det foreligger tungtveiende hensyn som taler for at Norge ikke bør benytte seg av reservasjonsadgangen i konvensjonens artikkel 6 nr. 3. De typer innretninger det her er tale om har et begrenset lovlig bruksområde, og kan brukes til å begå alvorlige straffbare handlinger. Datavirus og hackerverktøy kan volde betydelige skader og kostnader for samfunnet. De gjør det mulig å skaffe seg opplysninger av betydning for rikets sikkerhet og krenke viktige private og samfunnsmessige interesser.

Dersom Norge benytter reservasjonsretten, betyr det etter disse medlemmers syn at man i realiteten ikke vil kunne straffe en som gjør hackerverktøy tilgjengelig for andre på nettet, selv om man med sikkerhet kan si at dette verktøyet vil bli brukt til å begå ulike straffbare handlinger med lav oppdagelsesrisiko.

Disse medlemmer støtter derfor departementets syn om at det bør være straffbart å være i besittelse av passord og hackerverktøy, samt å gjøre slike innretninger tilgjengelige for andre. »

Komiteen fremmet deretter flertallets lovforslag til nytt straffebud, likelydende med straffeloven § 145b, som ble vedtatt. Flertallet hadde imidlertid på følgende måte også signalisert at man ønsket fortsatt arbeid med disse problemstillingene:

«Flertallet ber imidlertid om at arbeidet tilknyttet problemstillingen rundt forberedelseshandlinger og det å være i besittelse av «datavirus, hackerverktøy o.l» fortsetter.»

Det fremgår altså at lovgiver ønsket en fortsatt utredning av spørsmålet og at man ikke nødvendigvis ville anse seg bundet av det standpunkt som ble inntatt ved lovendringen i 2005. Problemstillingen er omfattet av mandatet, og som det har fremgått er spørsmålet nå utredet på nytt.

### *Flertallets syn*

Utvalget har som nevnt delt seg i synet på utkastet § 11. Flertallet bestående av medlemmene Rønning, Sellæg, Gulbrandsen og Christensen begrunner sitt standpunkt på følgende måte:

Utgangspunktet er at datakrimkonvensjonen artikkel 6 legger opp til at medlemsstatene skal straffe slike handlinger. Straffetrusselen skal virke preventivt slik at tilgjengeligheten av verktøy som gir ulovlig tilgang til datasystem reduseres. Når det blir vanskeligere å få fatt i denne typen verktøy reduseres også risikoen for å bli utsatt for datakriminalitet. I hvert fall antas dette å gjelde når gjerningspersonene er såkalte «script kiddies» (se kapittel 3.3.3), siden disse står for en stor del av den registrerte datakriminaliteten. Slike personer som mangler kompetanse til å programmere er avhengig av å skaffe seg verktøy fra andre, typisk via internett. Det antas derfor at straffebudet kan få en reell preventiv effekt for denne gruppen.

Utkastet § 11 er utformet slik at de objektive gjerningsvilkår gjelder konkrete konstaterbare forhold. Det er altså ikke tale om å kriminalisere utelukkende på grunnlag av den onde hensikt, jf. betraktningene om dette i NOU 2003:27 side 19 flg. For øvrig stilles det krav om forsett som er den vanlige skyldform etter loven. De forskjellige befatningsformer skulle ikke by på problemer ved praktiseringen av bestemmelsen, det vises til kommentarene i spesialmotivene.

Flertallet mener at det er straffverdig å spre verktøy som gir ulovlig tilgang til datasystem. Etter hva man har brakt i erfaring skjer dette i stor utstrekning på internett, hvor man tilbys program som enkelt kan lastes ned og utnyttes. I tillegg kan man bestille dertil egnet utstyr via nettsteder. For å effektivisere spredningsforbudet er det også nødvendig å ramme det å fremstille, modifisere, besitte og anskaffe denne typen verktøy (jf. utkastet § 11 første ledd annet punktum).

Flertallet mener at det er lite holdepunkt for at en bestemmelse som utkastet § 11 vil ha uheldige virkninger for lovlig datarelatert virksomhet. Det være seg for aktører i sikkerhetsbransjen eller for forskning og utvikling av datateknologi og tjenester. Det vises til at straffebudet på vanlig måte inneholder en rettsstridsreservasjon. Dessuten rammer det bare verktøy som er «særlig egnet» til å begå overtredelser som nevnt. Vilkåret «særlig egnet» innebærer at verktøyet må ha funksjonalitet som er spesielt hensiktsmessig for å begå de overtredelser som er nevnt i bestemmelsen. Exploits og piratdekoderkort er eksempler på verktøy som antas å oppfylle dette kriteriet.

Forsettvilkåret innebærer at gjerningspersonen må være klar over dette. Videre innebærer rettsstridsreservasjonen at det ikke blir tale om å straffe befatning med slike verktøy i vanlig lovlig virksomhet. Det vil for eksempel ikke være straffbart å anskaffe og benytte slike verktøy på eget datasystem. Dersom straffebudet leder til en generell reduksjon i spredning av verktøy som nevnt, også slik spredning som forestås av sikkerhetsbransjen på åpne kanaler på internett, er straffebudets preventive formål et stykke på vei oppnådd. Det antas at profesjonelle aktører i denne bransjen har mulighet for å organisere distribusjon av slike verktøy seg imellom uten at det nødvendigvis må skje over allment tilgjengelige kanaler, hvor verktøyene også kommer kriminelle miljøer i hende.

Flertallet mener at i lys av alle de sikkerhetsproblemer som forårsakes på grunn av den store tilgjengeligheten av skadelig dataprogram og utstyr, er tiden inne til at lovgiver gir et klart forbud mot dette. Utkastet § 11 ligger for øvrig i forlengelsen av den nevnte straffebud i straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd og § 53c. Flertallet er ikke kjent med negative virkninger av de nevnte regler, som skulle tilsi noen spesiell tilbakeholdenhet i forhold til utkastet § 11.

*Mindretallets syn*

Mindretallet, bestående av medlemmene Willassen og Taraldset er av den oppfatning at man ikke bør gjennomføre den nykriminalisering som utkastet § 11 innebærer. Mindretallet mener at bestemmelsen bør utgå. I stedet foreslår mindretallet at man opprettholder dagens rettstilstand ved at bestemmelsene i straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd og § 53c videreføres.

Mindretallet begrunner sitt standpunkt på følgende måte:

Datakrimkonvensjonens artikkel 6 legger opp til at medlemsstatene skal straffbelegge befatning med verktøy, herunder programvare, som kan benyttes til å begå straffbare handlinger etter datakrimkonvensjonens artikler 2-5. Disse artiklene omhandler ulovlig tilgang til datasystem (artikkel 2), dataavlytting (artikkel 3), datamodifikasjon (artikkel 4 og 5) og driftshindring (artikkel 5). Befatning omfatter produksjon, salg, anskaffelse for bruk, import, distribusjon eller annen form for tilgjengeliggjøring, samt besittelse. Det er et krav for straffbeleggelse etter artikkel 6 at befatningen skjer i den hensikt at verktøyet skal benyttes til å begå en av de straffbare handlingene som nevnt. Artikkel 6 inneholder også i nr. 1, a, ii, et krav om straffbeleggelse av befatning med tilgangsdata, se kapittel 5.7.4. Med unntak av spredning av tilgangsdata, kan medlemsstatene reservere seg mot innholdet i artikkel 6. Det er således gjort valgfritt hvorvidt man ønsker å implementere en slik bestemmelse som flertallet foreslår i utkastet § 11.

I forbindelse med delutredning I (NOU 2003: 27), drøftet Datakrimutvalget problemstillingen, og kom til at det ikke var tilrådelig å innføre et slikt straffebud. Utvalget la da til grunn at det dreier seg om forberedelseshandlinger som normalt er straffrie etter norsk rett. Straff er samfunnets skarpeste reaksjon mot uønsket adferd, og bør brukes med varsomhet. Særlig varsom bør man være med å kriminalisere forberedelseshandlinger. Slike handlinger krenker normalt ikke beskyttelsesverdige interesser, og det kan være usikkert om den straffbare handlingen som forberedes, vil bli gjennomført. Mindretallet slutter seg til denne vurderingen. Ser man bort fra besittelse av særlig farlige gjenstander, for eksempel plutonium og uran

(straffeloven § 152 a) eller sprengstoff (straffeloven § 161) er det normalt ikke straffbart å besitte gjenstander som kan benyttes til kriminelle formål, heller ikke om dette var hensikten med anskaffelsen. Med unntak av selvspredende dataprogram (se kapittel 5.7.6), mener mindretallet at den type verktøy som omtales i artikkel 6, neppe kan sies å være verktøy som i seg selv er spesielt skadelig eller farlige. Som det vil bli redegjort for i det følgende, er det hovedsaklig snakk om dataprogrammer som i tillegg til å kunne brukes til å begå straffbare handlinger som datainnbrudd, også kan benyttes til lovlige og nyttige formål.

Utkastet § 11 straffbelegger det å uberettiget anskaffe, fremstille, modifisere, besitte eller tilgjengeliggjøre dataprogram som er særlig egnet til å begå handlinger som er straffbare etter utkastet §§ 4-8, 10 og 13-14. For å forstå hvorfor dette blir et vidtrekkende straffebud, er det nødvendig å gå gjennom noen av de typer dataprogrammer dette gjelder.

### *§ 4 Ulovlig tilgang til datasystem*

Programmer for å skaffe seg ulovlig tilgang til datasystem finnes i flere kategorier. Det typiske eksemplet er såkalte «exploits» (omtalt i kapittel 3.4.1). Exploits kan benyttes til å skaffe seg ulovlig tilgang til datasystem, men kan også benyttes til å verifisere om spesielle sårbarheter finnes på en datamaskin.

Programmer for fjerninnlogging kan også sies å være egnet til å begå datainnbrudd, idet slike programmer kan benyttes til å logge seg på med andre brukernavn og passord. Det er neppe tvilsomt at den lovlige bruken av slike programmer er langt mer omfattende enn den ulovlige.

### *§§ 5 og 6 Data- og informasjonstyveri*

Programmer som er særlig egnet til å begå data- og informasjonstyveri inkluderer blant annet verktøy som avlytter nettverkstrafikk, ved å lagre dataene som passerer på nettverket. Programmet tcpdump er et eksempel på et slikt program. Dette programmet distribueres sammen med de fleste UNIX-operativsystemer (for eksempel Linux), og er mye brukt i forbindelse med utvikling av nettverksprogrammer.

### *§§ 7 og 13 Datamodifikasjon og driftshindring*

Programmer som er særlig egnet til å begå datamodifikasjon eller driftshindring omfatter en rekke forskjellige programmer som kan kalles skadeverksprogrammer. En stor kategori av slike programmer, som utfører spesielt stor skade er programmer som sprer seg selv ved å skaffe seg ulovlig tilgang til datasystemer. Slike programmer er omtalt i kapittel 3.4.8, og befatningen foreslått kriminalisert som selvstendig straffbar handling i utkastet § 12. Mindretallets reservasjon omfatter som nevnt ikke utkastet § 12.

Ser man bort fra selvspredende programmer, kan det være tale om programmer som er spesiallaget for å gjøre modifikasjoner på en bestemt maskin (trojaner), eller det kan være programmer som er laget for å sende store datamengder mot andre datamaskiner (tjenestenektprogrammer).

### *§ 14 Masseutsendelse av elektroniske meldinger*

Det kan finnes en rekke forskjellige programmer som vil være velegnet for masseutsendelse av elektroniske meldinger. Vanlige e-postprogrammer er eksempler på slike, men også programmer som er spesiallaget for masseutsendelse av e-post eller sms.

Etter mindretallets vurdering er det etter flertallets forslag usikkert hvilke programmer som vil rammes av den foreslåtte bestemmelsen og hvilke som ikke vil det. Hva som ligger i «særlig egnet», vil det nok herske delte meninger om. Det er ikke tvil om at det finnes mange programmer som er særlig egnet til å begå straffbare handlinger som også har nyttige funksjoner. Det er snakk om programmer som finnes åpent tilgjengelig på databaser på internett, og som i flere tilfeller følger med som en integrert del av annen programvare, for eksempel sikkerhetsprogrammer og operativsystemer.

Mindretallet frykter at en slik omfattende straffbelegging av befatning med slik programvare som flertallet legger opp til, vil ha en betydelig kjølende effekt på IT-bransjen i Norge. Dersom man engasjerer seg i utvikling av programvare som viser seg å også være særlig egnet til å begå straffbare handlinger etter datakrimkapitlet, risikerer man å bli straffet for dette. Det er ikke mulig å drive med datasikkerhetsvirksomhet uten å ha befatning med dataprogrammer som er særlig egnet til å begå datakriminalitet. Det vil være lett (for eksempel fra en konkurrent) å hevde at et datasikkerhetsverktøy også kan benyttes til å muliggjøre datainnbrudd, og at dette har vært en del av motivasjonen ved fremstillingen. Dermed vil man kunne bli mistenkeliggjort og utsatt for strafforfølgning (med rette eller urette) for å ha begått en aktivitet som samfunnet i utgangspunktet ønsker og oppmuntrer til. Det kan hevdes at

bestemmelsen i realiteten pålegger datasikkerhetsbransjen en plikt til å være ekstra varsomme og å dokumentere at den virksomheten man driver med ikke på noe tidspunkt er motivert av et ønske om å muliggjøre at andre kan begå straffbare handlinger. En slik plikt kan nok føles byrdefull, såfremt konkurrentene i utlandet ikke har noen tilsvarende plikt.

Mindretallet forstår flertallets ønske om å gjøre verktøy som kan benyttes til datakriminalitet vanskeligere tilgjengelig. Det er ikke tvilsomt at når slike verktøy er lett tilgjengelig blir det lettere å begå datainnbrudd på datamaskiner som ikke er sikret mot kjente sårbarheter. Mindretallet vil imidlertid peke på at den samme tilgjengeligheten gjør det mulig for den som vil beskytte seg mot slike datainnbrudd å finne ut hvilke metoder som benyttes. Ved at verktøyene er tilgjengelige, kan datasikkerhetsbransjen avdekke hvilke sårbarheter som utnyttes og beskytte seg ved å fjerne sårbarhetene. Flertallets forslag medfører at det blir belagt med straff å tilgjengeliggjøre verktøy som benyttes til datainnbrudd. Formålet med denne straffbeleggelsen er å gjøre verktøy for datainnbrudd mindre tilgjengelig, slik at det blir vanskeligere å begå denne type handlinger. Mindretallet frykter at dette vil føre til at metodene som kriminelle bruker for å begå datainnbrudd ikke blir kjent for datasikkerhetsmiljøet, slik at man ikke kan beskytte datamaskiner mot de verktøyene som de kriminelle bruker. Resultatet kan altså bli stikk motsatt av det man ønsket å oppnå: Datasikkerheten vil bli dårligere fordi det ikke lenger vil være mulig å beskytte systemene mot de datainnbruddsmetoder som benyttes. Dermed vil det ikke lenger være mulig å beskytte datasystemer med et høyt sikkerhetsbehov mot kjente angrep, slik det er i dag.

Flertallets forslag til § 11 kriminaliserer tilgjengeliggjøring av dataprogram som er særlig egnet til å begå datakriminalitet. Enhver form for tilgjengeliggjøring rammes, enten det er massiv distribusjon eller tilgjengeliggjøring ved at man gir verktøyet videre til en annen person. Utkastet § 1 bokstav b definerer dataprogram som

> «Data i form av en sekvens av instruksjoner som kan utføres i et datasystem, herunder kildekode.»

En konsekvens av flertallets forslag er dermed at også tilgjengeliggjøring av beskrivelser av virkemåten til programmer som er «særlig egnet» til å begå datakriminalitet vil rammes. Kildekode er en beskrivelse av virkemåten til et dataprogram, i en form som er lett forståelig for mennesker og som er eller kan oversettes til et kjørbart dataprogram. En slik beskrivelse er som en prosatekst som beskriver virkemåten til programmet. Teksten følger som enhver tekst grammatiske og syntaktiske regler, som i tilfelle kildekode er definert i programmeringsspråket som er benyttet. På bakgrunn av dette ønsker mindretallet å påpeke forslagets innvirkning på ytringsfriheten. Det er fare for at utkastet § 11 innebærer et utilbørlig inngrep i retten til å fremsette ytringer som inneholder beskrivelser av omgåelse av sperrer på datasystemer, i form av kildekode. Det er ikke straffbart å fremsette slike ytringer i dag. Mindretallet er bekymret for at § 11 utgjør en begrensning i ytringsfriheten. I så fall må dette begrunnes i tungtveiende hensyn som er klart definerte, jf. drøftelsen i kapittel 7.2. Mindretallet mener at det verken foreligger eller er anført slike tungtveiende hensyn. Derimot er det som nevnt tungtveiende hensyn som taler mot å straffbelegge slike ytringer.

Mindretallet er etter dette kommet til at utkastet § 11 ikke bør implementeres i straffeloven og at Norge fortsatt bør reservere seg mot datakrimkonvensjonens artikkel 6 for så vidt gjelder slike verktøy som er nevnt i artikkel 6 nr. 1, b og nr. 1, a, i. Dette er i samsvar med konklusjonen i Datakrimutvalgets delutredning I (NOU 2003: 27).

Flertallet foreslår at straffeloven § 262 første ledd og åndsverksloven § 53a annet ledd og § 53c inkorporeres i utkastet § 11. For å unngå å utvide kriminaliseringen av dataprogram og utstyr som nevnt, foreslår mindretallet at straffeloven § 262 første ledd og åndsverksloven § 53a andre ledd og § 53c, opprettholdes som egne bestemmelser. Straffeloven § 262 første ledd kan eventuelt innarbeides i datakrimkapitlet.

### 5.7.6 Selvspredende dataprogram

*De legislative hensyn*

Utvalget går enstemmig inn for å kriminalisere befatning med selvspredende dataprogram. Begrunnelsen er at selve den egenskap at det sprer seg selv er så skadelig at det bør være straffbart å fremstille, modifisere, anskaffe og spre det. Det preventive formål er med andre ord vesentlig. Den rene besittelse foreslås ikke kriminalisert siden problemets karakter nettopp består i at programmet legger seg på fremmede vertsmaskiner, slik at svært mange kommer i besittelse av denne type program, om enn ufrivillig. Det vises til de nærmere overveielser omkring besittelse nedenfor.

Den selvspredende egenskapen innebærer at spredningen ikke lar seg styre eller begrense når programmet først er tilgjengeliggjort. Det finnes neppe legitime grunner til å fremstille dataprogrammer hvor spredningen ikke lar seg kontrollere. De skadelige konsekvenser er godt dokumentert, se kapittel 3.4.8. Nødvendige beskyttelsestiltak må skje defensivt, det vil si ved å ta i bruk antivirusfiltre og programvare som er sikkerhetsmessig oppdatert, slik at datasystemet ikke skal kunne la seg infisere av det selvspredende programmet. Karakteristikken «virus» som ofte benyttes på dataprogram med selvspredende egenskap, er for så vidt dekkende for å beskrive hva slags problem dette utgjør. Bare kostnadene som følger med anskaffelse og bruk av nødvendige sikkerhetstiltak representerer enorme beløp. Dette har for så vidt skapt et stort marked for datasikkerhetsprodukter og -tjenester, men representerer egentlig unødvendige kostnader.

Dataprogram som ikke har annen egenskap enn at det ukontrollert sprer seg selv, er trafikk i nettet som bør stanses. De hensyn som gjør seg gjeldende er langt på vei de samme som kan anføres mot spam (søppelpost), nemlig at det utgjør en belastning og ikke har et selvstendig formål som begrunner eller rettferdiggjør spredningen, se merknadene om spam i kapittel 5.6.6.

Ofte har selvspredende dataprogram i tillegg slik funksjonalitet at de skaper en sårbarhet eller annen uønsket effekt på vertsmaskinen. Dette rammer systemintegriteten, noe som anses som en meget negativ effekt, se nærmere om hensynet til systemintegriteten i kapittel 4.6.2. Det har således forekommet at slike program lager «bakdør» på datasystemer. Deretter kan man ved bruk av elektronisk kartlegging identifisere hvilke datasystemer som på denne måten er blitt sårbare for inntrengning og misbruk, og utnytte dem deretter. Slik elektronisk kartleggingsvirksomhet er for øvrig foreslått kriminalisert, jf. utkastet § 2.

Det har også vært spredt selvspredende dataprogram som foruten å spre seg selv til andre datasystem, har kopiert seg selv kontinuerlig på vertsmaskinen slik at kapasiteten blir for hardt belastet og vertsmaskinen slutter å fungere. Ytterligere har det forekommet at selvspredende dataprogram har kopiert innhold fra vertsmaskinene og lagt det åpent tilgjengelig på internettservere. Disse egenskapene krenker hensynene til integritet, tilgjengelighet og konfidensialitet.

Uavhengig av om dataprogrammet har funksjonalitet utover selvspredningen, er konsekvensen at det uberettiget legger seg på en vertsmaskin og at det skjer en modifikasjon i programutrustningen eller andre data på denne. Det kan også skapes så stor belastning både på datasystemene og i selve nettet at det kan gå drastisk ut over driften. Forbudet mot selvspredende dataprogram har følgelig et nært slektskap med reglene i utkastet § 4 om ulovlig tilgang til datasystem, utkastet § 7 om datamodifikasjon og utkastet § 13 om driftshindring. Dessuten gjør til dels de samme hensyn seg gjeldende som for spam, jf. utkastet § 14.

### *Overveielser vedrørende de straffbare befatningsformer og skyldform*

Utvalget går inn for å straffe fremstilling, modifisering, anskaffelse, tilgjengeliggjøring og initiering av spredning av selvspredende dataprogram. Det vises til merknadene i de spesielle motivene om disse alternativene. Ytterligere to befatningsformer har vært vurdert, nemlig besittelse og markedsføring, sammenlign de tilsvarende alternativene i utkastet §§ 10 og 11.

Utvalget har ikke foreslått å kriminalisere besittelse av selvspredende dataprogram. For det første er selve problemet manifestert ved at mange er i uønsket besittelse av programmet, og kanskje uten selv å være klar over det. De har mottatt programmet elektronisk uten å ha foretatt noen aktiv handling. Det kan synes betenkelig å sette straff for den vanligste befatningsformen, hvor det hele da avhenger av skyldkravet. Dessuten kan det tenkes å oppstå tilfeller hvor det virker urimelig å anvende straff når årsaken til at besittelsen har oppstått ikke har sammenheng med noen straffverdig handling hos innehaveren av vertsmaskinen. Besittelse som følge av aktive handlinger som fremstilling og anskaffelse, rammes uansett indirekte ved at de nevnte forutgående handlinger er gjort straffbare. Grunnleggende sett vil besittelsen i de tilfelle den har oppstått ufrivillig ikke kunne anses å være rettsstridig. Det synes heller ikke å foreligge noe større behov for å anvende straff i slike tilfelle.

Det foreslås heller ikke straff for å markedsføre selvspredende dataprogram, siden det karakteristiske ved programmet er at det sprer seg selv. Verken markedsføring i seg selv eller det å kriminalisere eventuell markedsføring, ses å tjene noe fornuftig formål.

Utvalget har sett nøye på de straffalternativ som gjelder *spredning* av selvspredende dataprogram. Et slikt program kan spres fra et sted til et annet uten at den selvspredende funksjonen nødvendigvis er iverksatt. I et slikt tilfelle er det tale om spredning uten at det selvspredende dataprogrammet er startet opp. Som eksempel kan man tenke seg en programmerer som lager et selvspre-

dende dataprogram som han lagrer på en cd-plate. Dersom han gir cd-platen til en kollega er programmet spredt, men selvspredningen er ikke iverksatt fordi det krever at programmet startes opp. Det å starte programmet leder med nødvendighet til at den selvspredende egenskapen aktiviseres, det vil si at man mister kontroll med spredningen. Denne handlingen kan kalles å initiere spredning.

Utvalget mener at begge de nevnte handlinger bør være straffbare. Det skadeligste er å starte opp et program med selvspredende funksjonalitet siden man da må regne med å miste kontrollen over det. I det minste er risikoen for tap av kontroll svært stor. Utvalget mener derfor at det må kreves stor grad av aktsomhet i omgang med slikt dataprogram og at det å starte det opp bør være straffbart også i sin grovt uaktsomme form.

I denne sammenheng er det naturlig å nevne hensynet til forskning. Det er et viktig rettspolitisk hensyn at forskningen ikke skal bli skadelidende følge av den strafferettslige regulering. Dette hensynet tillegges derfor generelt stor vekt ved rettsstridsvurderingen. Men for så vidt gjelder selvspredende dataprogram er skadevirkningen av spredning så stor og veldokumentert at det er vanskelig å se hensyn som gjør det legitimt å fremstille eller initiere slikt program, selv om det skjer i et forskningsmiljø. Det at en aktivitet er eller kaller seg forskning, er i dette henseende ikke nødvendigvis fritakende for straff.

Utvalget går ikke inn for å anvende grov uaktsomhet som skyldform for andre befatningsformer enn initiering av spredning. Dette har sammenheng med et annet rettspolitisk utgangspunkt, nemlig at straffebudene skal verne om den alminnelige borgers behov for beskyttelse og at man må unngå å utforme reglene slik at de blir urimelig byrdefulle for borgerne. Imot dette kan det fremholdes at ved å anvende en skjerpet skyldform kunne man oppnå en viss preventiv effekt og redusere det omfattende virusproblemet. Utvalget mener imidlertid at det er fare for at et vilkår om grov uaktsomhet vil kunne få for stor slagvidde for alternativene anskaffelse og tilgjengeliggjøring av selvspredende dataprogram.

Overfor fremstillingsalternativet er grov uaktsomhet uansett lite praktisk, siden man vanskelig kan tenke seg at en programmerer uforvarende skulle skrive kildekode som inneholdt instruksjoner om selvspredning. Anskaffelse og tilgjengeliggjøring (spredning) derimot, kan skje uforvarende dersom man ikke har sikret seg mot å bli utsatt for datavirus. Dette krever at man tar i bruk antivirusprogrammer og sørger for jevnlig oppdatering av programutrustningen. Borgerne er i stor grad avhengig av profesjonelle tjenesteytere for å kunne sikre seg. Utvalget mener at ansvar for å tilrettelegge for sikker bruk av datatjenester og elektronisk kommunikasjon først og fremst bør påhvile de profesjonelle aktører. Utvalget deler således ikke Sikkerhetsutvalgets utgangspunkt om at det påhviler et eget ansvar for den enkelte bruker med hensyn til dette problemet, jf. uttalelser og anbefalinger i utredningen i NOU 2006: 6 «Når sikkerheten er viktigst» side 108. Utvalget går derfor inn for å anvende forsett som skyldform for alle straffalternativene i utkastet § 12, med unntak av det å initere spredning av selvspredende dataprogram.

Gjerningsbeskrivelsen i utkastet § 12 er fordelt på to ledd, hvor de forsettlige overtredelsesformer er plassert i første ledd, mens det å initiere spredning av selvspredende dataprogram er plassert i annet ledd. Initieringsalternativet foreslås altså å være straffbart både i forsettlig og grovt uaktsom form, se også utkastet § 17.

*Strafferammer*

Som nevnt legges det til grunn at den selvspredende egenskapen i seg selv er tilstrekkelig grunn for kriminalisering. Den ordinære strafferammen for straffbar befatning med denne typen selvspredende dataprogram foreslås satt til bøter eller fengsel inntil 1 år. Dersom programmet har annen skadelig funksjonalitet i tillegg er det grunn til å anvende strengere straff, og det foreslås at strafferammen for slike tilfeller øker til fengsel inntil 3 år. For grov overtredelse foreslås strafferammen satt til fengsel inntil 6 år.

## 5.8 Databedrageri og kontomisbruk

### 5.8.1 Innledning

Utvalget har vurdert databedrageribestemmelsen. Etter datakrimkonvensjonen artikkel 8 er Norge forpliktet til å ha straffebud som rammer forsettlig handling som

> «påfører andre tap av eiendom gjennom
> a) innlegging, endring, sletting eller utilgjengeliggjøring av elektroniske data,
> b) inngrep som forstyrrer et datasystems drift,
> i den svikaktige eller uredelige hensikt å skaffe seg eller andre urettmessig økonomisk vinning.»

I delutredning I konkluderte Datakrimutvalget med at den gjeldende bestemmelsen i straffeloven § 270 første ledd nr. 2 alene oppfyller hele forpliktelsen etter artikkel 8, og foreslo følgelig ikke noen endring i bestemmelsen. Alternativet i artikkel 8 b,

anses å ha liten selvstendig betydning ved siden av alternativet i bokstav a. Uansett forutsettes det at det skjer forstyrrelser i prosessene på datasystemet. Dette dekkes av alternativene i den gjeldende databedrageribestemmelsen.

I delutredning VII kapittel 9.18 side 380, foreslås bedrageribestemmelsen videreført i utkastet § 32-1 om bedrageri. Det opplyses kort at man foreslår «videreført her både den tradisjonelle bestemmelsen om bedrageri og straffebudet mot databedrageri». Utformingen av databedrageribestemmelsen er ikke kommentert.

### 5.8.2 Hjemmel og historikk

Datakrimutvalget har sett på databedrageribestemmelsen på nytt, i lys av erfaringene med bruken av bestemmelsen og sammenhengen med de øvrige bestemmelsene i lovforslaget.

Databedrageribestemmelsen lyder som følger, jf. straffeloven § 270 første ledd nr. 2:

> «For bedrageri straffes den som i hensikt å skaffe seg eller andre en uberettiget vinning [...]
>
> 2) ved bruk av uriktig eller ufullstendig opplysning, ved endring i data eller programutrustning eller på annen måte rettsstridig påvirker resultatet av en automatisk databehandling, og derved volder tap eller fare for tap for noen.»

Databedrageribestemmelsen ble tatt inn i straffeloven i forbindelse med lovrevisjonen om datakriminalitet i 1987. Bestemmelsen var begrunnet i et behov for å dekke tapsvoldende manipulasjoner av datasystem som ble begått i vinnings hensikt. Man mente at manipulasjonen var beslektet med et ordinært bedrageri. Men siden bedrageribestemmelsen oppstiller krav om «villfarelse», det vil si en subjektiv tilstand som bare kan oppstå hos et menneske, kunne den ikke anvendes overfor manipulasjon av datasystemer. Det var derfor behov for en særlig bestemmelse som rammet dette.

### 5.8.3 Problemstillinger

Straffeloven § 270 første ledd nr. 2 angir tre alternative misbruksformer, henholdsvis:

- «ved bruk av uriktig eller ufullstendig opplysning»,
- «ved endring i data eller programutrustning»,
- «eller på annen måte».

I tillegg kreves det at handlingen «rettsstridig påvirker resultatet av en automatisk databehandling» og derved volder økonomisk tap eller fare for tap.

Alternativene er delvis overlappende, men det typiske er at første alternativ overtres ved å tilføre datasystemet opplysninger det ikke hadde fra før, annet alternativ ved å foreta endringer i data eller programutrustning som allerede er på datasystemet, og tredje alternativ, for eksempel ved å slette data, se Bratholm og Matningsdal: Straffeloven kommentarutgave side 724. Misbruk av kredittkort vil derfor kunne rammes etter første eller tredje alternativ. Til illustrasjon av bestemmelsen kan det vises til saksforholdet i noen Høyesterettsavgjørelser.

- Rt. 1990 side 955. Domfelte hadde bokført fiktive bilag som leverandørgjeld i arbeidsgiverens databaserte regnskapssystem, samtidig som de ble bokført som utgående moms. Fakturaene kom til utbetaling over domfeltes lønnskonto.
- Rt. 1991 side 532 (BBS-dommen). Dommen gjaldt forsøk på databedrageri. De to domfelte hadde endret kontoopplysninger i datasystemet til Bankenes Betalingssentral, ved å erstatte kontonumrene til lokale trygdekontorer med sine egne konti. Den månedlige overføringen fra Rikstrygdeverket til de lokale trygdekontorene ble derfor i stedet styrt til de domfeltes konti i utlandet. Gjennomføringen lyktes ikke siden varslingssystemet i BBS ba om kontroll på en meget stort delbeløp (kr. 512 millioner) som inngikk i det totale beløpet som var til overføring (kr. 889 millioner), med den følge at bedrageriforsøket ble oppdaget.
- Rt. 1994 side 740. Domfelte var ansatt i en bank som kunderådgiver med bevilgningsfullmakt. Hun åpnet fem spesifiserte konti med seg selv som tilskriveradressat, og på en sjette konto endret hun tilskriveradressen med seg selv som adressat. Hun innvilget kreditter og overtrekkslimiter på kontiene. Ved girobelastninger, kontouttak og overføringer disponerte hun kontoene slik at det oppsto betydelig negativ saldo. Banken led tap eller fare for tap for et tilsvarende beløp.
- Rt. 1995 side 1872 (pinkodekjennelsen). Domfelte hadde skaffet seg adgang til og aktivisert dataprogrammer i telefonselskaper eller deres abonnenters datamaskiner. De ble derved påført tap i form av uriktig tellerskrittbelastning. Dermed påvirket han resultatet av en automatisk databehandling.

### 5.8.4 Behovet for en ny lovbestemmelse

De mest praktiske tilfeller av databedrageri er uberettiget bruk av andres kredittkort eller debetkort i situasjoner hvor slike kort eller kortinformasjon

benyttes i maskinelle prosesser og kortet ikke kontrolleres av mennesker. Det fremgår imidlertid ikke uttrykkelig av lovteksten at disse situasjonene faller inn under bestemmelsene om databedrageri.

For å klargjøre dette, foreslår utvalget en ny lovbestemmelse om kontomisbruk. Bestemmelsen omfatter imidlertid langt mer enn misbruk av kort. Når det er utstedt et kort, foreligger det i alle profesjonelle tilfeller et kontoforhold som er knyttet til kortet. Det er således den uberettigede bruken av kontoen om representerer databedrageriet. Utvalget foreslår derfor en generell lovbestemmelse som skal ramme alle former for misbruk av konto – uavhengig av om det er knyttet kort eller annen representasjon til kontoforholdet eller ikke.

Bruk av stjålet kort eller kortopplysninger rammes i dag av databedrageribestemmelsen første alternativ om «bruk av uriktig eller ufullstendig opplysning». Dette kan synes noe kunstig fordi opplysningene som avgis, kredittkortnummeret og sikkerhetskoden, isolert sett er riktige. Derimot forties det ikke uvesentlige forhold at man ikke er berettiget til å bruke kortet. Man har dog muligheten for å anvende det siste alternativet i straffeloven § 270 første ledd nr. 2, nemlig «på annen måte». I rettspraksis presiseres det ikke bestandig hvilket alternativ som er anvendt i det konkrete tilfellet. Det antas imidlertid at det kan være klargjørende med et eget straffebud som tar sikte på slike former for misbruk. Det er en krenkelse som forekommer hyppig og som med fordel kan komme klarere til uttrykk i loven.

Det kan reises spørsmål om de tre straffalternative i straffeloven § 270 nr. 2, dekkes av andre straffebestemmelser. Uberettigete endringer på datasystemer m.v. kan rammes som dataskadeverk, jf. straffeloven § 291, og som datamodifikasjon jf. utkastet § 7. Endringer kan også etter omstendighetene rammes som uberettiget bruk av datasystem, jf. straffeloven §§ 261 og 393, og utkastet § 8. Dette poenget er også fremhevet i Explanatory Report til datakrimkonvensjonen, punkt 87, hvor det står: «The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles». Det er imidlertid klart at misbruk i form av avgivelse av uriktige opplysninger til datasystem ikke omfattes av utkastet §§ 7 og 8. Ofte gis informasjonen på en måte som i utgangspunktet er rettmessig, for eksempel ved at webskjemaer fylles ut og sendes til en nettbutikk. Innholdet som formidles er imidlertid uriktig idet brukeren ved å sende inn skjemaene utgir seg for å ha rett til å bruke andres konti. I slike situasjoner kan ikke bestemmelsene om datamodifikasjon og uberettiget bruk av datasystem benyttes. Det vil derfor være behov for en bestemmelse som knytter seg til det sentrale element i handlingen, nemlig misbruk av andres konto.

### 5.8.5 Kontomisbruk

Kontomisbruk foreligger når noen uberettiget benytter en konto som tilhører en annen.

*Hva er en konto?*

En konto foreligger når noen har bestemte rettigheter hos andre basert på et avtaleforhold. Begrepet konto er søkt definert i utkastet § 16 annet punktum. Etter definisjonen er det et vilkår at informasjon om rettighetene er lagret elektronisk. Det er her tenkt på at lagringen skjer i datasystemer som den forpliktede har rådighet over. Slik elektronisk lagring skjer i praktisk talt alle profesjonelle forhold i dag, så denne delen av definisjonen innebærer knapt noen praktisk begrensning i slike forhold.

Rettighetene det er snakk om, er rettigheter av økonomisk art. Det kan være tale om et innskudd av penger som kan benyttes til for eksempel varekjøp eller annet. Et eksempel på en slik konto vil være en bankkonto. Det kan videre være tale om en rett til kreditt. Kredittavtale med et kredittkortselskap er et praktisk eksempel på en slik konto. Det samme gjelder konti som faller inn under lov om e-pengeforetak av 13. desember 2002 § 1 (for eksempel en PayEx-konto). Rettighetene kan imidlertid bestå av annet enn penger, for eksempel rett til å motta tjenester. Et eksempel på en slik rettighet er retten til en flyreise. Når en elektronisk flybillett kjøpes mot forskuddsbetaling, vil det foreligge en rett til reisen for kjøperen som er lagret i flyselskapets datasystem. Også dette er en konto. Andre slike konti er konti som gir rett til et visst antall bussreiser eller et visst antall passeringer av veibommer. I praksis finnes det et stort antall varianter av slike konti. For at de skal falle inn under lovutkastet, er imidlertid kravet at rettighetene som er knyttet til kontoforholdet har økonomisk verdi.

En konto på en nettside som tilbyr gratis tjenester og hvor alle kan registrere seg som brukere, faller dermed utenfor definisjonen. Denne tjenesten har ikke økonomisk verdi. Motsatt forholder det seg med en konto på et betalingsbelagt nettsted som tilbyr informasjonssamfunnstjenester, for eksempel rett til å gjøre oppslag i et elektronisk leksikon. Ytes det betaling i tilknytning til bruken, har bruksrettigheten økonomisk verdi. Det karakteristiske er her at det leveres en tjeneste mot betaling knyttet til et løpende kontoforhold.

Kontoforhold er som regel knyttet til en navngitt fysisk eller juridisk person. Et kontoforhold med et kredittkortselskap med tilknyttet kredittkort er alltid knyttet til en bestemt rettighetshaver. Det kan imidlertid også tenkes anonyme konti som bare er knyttet til for eksempel en nummeridentifikasjon, pinkode eller et ihendehaverbevis. Et eksempel på slike konti er anonyme PayEx-konti (som kan kjøpes anonymt for et begrenset beløp). Også de anonyme konti er ment omfattet av utvalgets lovforslag.

Noen kontoforhold er løpende og andre gjelder engangsforhold. Et løpende kontoforhold er for eksempel en konto som gir løpende rett til kredittkjøp på en netthandel. En engangskonto kan for eksempel være retten til en bestemt flyreise på en bestemt dato. Begge typer konti er i utgangspunktet ment omfattet av lovforslaget.

Det er ofte knyttet fysiske representasjoner til slike konti. De mest typiske eksemplene på dette er kredittkort eller debetkort. De mest typiske eksemplene på kontomisbruk er derfor misbruk av andres kredittkort eller debetkort. Det er imidlertid intet krav at det skal være fysiske representasjoner knyttet til kontoforholdet.

I noen tilfeller er all informasjon om rettighetenes omfang og bruk lagret i en fysisk representasjon som innehaveren besitter. Det føres da ikke separat regnskap for innholdet og bruken av rettighetene andre steder. Armbånd med elektronisk brikke som gir rett til ytelser inntil et visst beløp, eventuelt adgang til visse steder eller begivenheter, er ofte i denne kategorien. Slike armbånd brukes i dag blant annet som oppgjørsmetode i svømmehaller og på festivaler. Det samme gjelder visse former for reisekort, for eksempel kort som gir adgang til et visst antall reiser med t-banen. Misbruk kan i så fall «tømme» representasjonen for verdi. Det karakteristiske er da at representasjonen ikke er knyttet til person og gir begrensede økonomiske rettigheter. Det er i slike tilfeller mest nærliggende å anvende bestemmelsene om tyveri og underslag på tredjemanns rettsstridige borttakelse eller tilegnelse av slike representasjoner. Det er derfor avgrenset mot slike tilfeller i forslaget til § 16 annet ledds annet punktum.

*Hva er misbruk?*

Misbruk vil foreligge dersom noen benytter en konto som tilhører en annen. Lovforslaget tar ikke sikte på bruk av egen konto i strid med avtaleforholdet. Bruken av kontoen må være uberettiget og skje forsettlig. Bruken må skje ved at det avgis opplysninger til et datasystem. Videre er det, i likhet med det som gjelder for bedrageribestemmelsene, i forslaget et vilkår at det voldes tap eller fare for tap for noen. Det er uten betydning om dette er den som kontoen er opprettet hos (for eksempel kredittkortselskapet), kontoinnehaveren, den som kontorettighetene søkes anvendt hos (for eksempel nettbutikken hvor kontoen søkes benyttet til betaling) eller andre. Som det fremgår, er det etter forslaget intet vilkår at det har oppstått tap. Det er tilstrekkelig at det forelå fare for tap.

*Plassering av lovforslaget.*

Utvalgets lovforslag er satt inn som § 16 i datakrimkapitlet. I motsetning til § 15 i forslaget, gjelder § 16 mange forhold som ikke spesielt er knyttet til data og datasystemer, selv om det som nevnt ovenfor er et vilkår i lovforslaget at informasjon om rettighetene er lagret elektronisk og at misbruket skjer ved at det avgis opplysninger til et datasystem. Det er derfor mulig at bestemmelsen alternativt kan plasseres sammen med bedrageribestemmelsene i straffeloven.

*Særlig om bruk av stjålet kort eller kortopplysninger*

Bruk av stjålet kredittkort blir ofte kalt kredittkortbedrageri. Språkbruken er ikke helt treffende. Ved bruk av kortet skjer en belastning som leder til at medkontrahenten i utgangspunktet får oppgjør ved at vedkommende får en fordring mot kredittkortselskapet. Den som bruker kortet pretenderer uriktig at han er rette innehaver av kortet, eller i det minste er berettiget til å bruke det. Denne pretensjonen har neppe betydning for medkontrahenten ved rent automatiserte oppgjør, som det her ofte er tale om, for eksempel når kortet benyttes på internett. Sikkerhetsmekanismen i transaksjonen er bruk av sikkerhetskode, og denne skal forutsetningsvis bare rette innehaver kunne disponere. Det kan for eksempel være en pinkode (noe han vet) eller et autogenerert passord (noe han har). Bruk av stjålet kort er en krenkelse overfor rette innehaver av kortet, eventuelt kortselskapet, men også medkontrahenten kan lide tap, dersom kortselskapet nekter å gjennomføre oppgjøret, til tross for at medkontrahenten allerede har levert ytelsen. Det kan også tenkes at kortselskapet fremsetter tilbakebetalingskrav (såkalt «charge back»). Også i dette tilfellet vil medkontrahenten lide tap. Misbruket av kortet vil derfor være til ulempe for alle de tre impliserte.

Bruk av falsk kort skal etter lovforslaget bedømmes på samme måte som bruk av stjålet kort. Bruk av stjålet eller falsk kort innebærer krenkelse av

autentiseringsrutiner og kan anses som en økonomisk form for identitetstyveri (Dette tilfellet faller ikke inn under utkastet § 15, se kapittel 5.6.7).

Slikt kortmisbruk kan også utøves uten at kortet besittes av gjerningspersonen rent fysisk. Det er tilstrekkelig at gjerningspersonen har de opplysninger som fremgår av kortet. Ved transaksjoner på internett er det tilstrekkelig å avgi opplysning om kortnummer, navn på innehaver, utløpsdato og sikkerhetskode. Slike opplysninger kan versere i kriminelle miljøer og misbrukes. Den som er direkte utsatt for «bedrageriet» er medkontrahenten, siden aksepten av transaksjonen skjer på hans side. Men også kortinnehaverens og kortselskapets interesser er krenket på straffverdig måte.

Når urette vedkommende benytter debetkort eller andre representasjoner eller informasjon som er nødvendig for å misbruke en konto knyttet til representasjonen, blir problemstillingen den samme som beskrevet ovenfor i forhold til kredittkort.

*Forholdet til gjeldende rett*

Et straffebud om kontomisbruk bør komme til anvendelse uansett hva motytelsen består i. Etter gjeldende rett skal kortsvindel bare bedømmes som databedrageri når motytelsen består i noe annet enn kontanter eller varer. Når motytelsen består i gjenstander som kan «borttas» kommer nemlig tyveribestemmelsen til anvendelse i stedet. Dette følger i dag av sikker rett, se blant annet Rt. 1997 side 1771 med henvisninger til forarbeider og rettspraksis. Det vises også til Sunde 2006 «Lov og rett i cyberspace» kapittel 5.6.4 om disse problemstillingene. Utvalgets forslag innebærer derfor en endring i forhold til gjeldende rett.

Hvilken form motytelsen har, om det er et dataprodukt eller en nyhetstjeneste levert over internett, kontanter fra minibank eller bensin fra en bensinautomat, bør ikke ha noen betydning i forhold til et nytt straffebud om kontomisbruk. Det karakteristiske ved handlingen er det økonomiske identitetstyveriet. Karakteren av motytelsen er i så henseende uvesentlig. Det er imidlertid en forutsetning at kortet er benyttet og «akseptert» direkte av en datamaskin. Dersom et stjålet kort benyttes i en butikk eller drosje og kontrolleres av et menneske, skal den alminnelige bedrageribestemmelsen fortsatt anvendes, jf. straffeloven § 270 første ledd nr. 1.

*Overbelastning av eget kort eller konto*

En annen form for kortmisbruk består i at rette innehaver uberettiget overbelaster kortet. Dersom ytelsen består i kontanter eller varer som kan borttas, skal handlingen etter gjeldende rett bedømmes som tyveri, jf. Rt. 1982 side 1816, Rt. 1990 side 17 og Rt. 1995 side 1652. Utvalgets forslag omfatter ikke slike former for misbruk, og det foreslås her ingen endringer i gjeldende rett.

### 5.8.6 Bør straffeloven § 270 første ledd nr. 2 videreføres?

Slik databedrageribestemmelsen i dag er utformet, fremstår den som komplisert og relativt lite brukt. Videre er det spørsmål om hvor hensiktsmessig det er å anvende vilkåret om å påvirke «resultatet av en automatisk databehandling», som iblant kan by på tvil.

Ved en eventuell gjennomføring av reglene i lovforslaget vil betydningen av databedrageribestemmelsen uansett reduseres vesentlig. Det er imidlertid mulig å finne eksempler på tilfeller som ikke dekkes av reglene i lovforslaget. Dette indikerer et behov for databedrageribestemmelsen også i fremtiden. Man kan for eksempel tenke seg at kostbare varer påføres klistrelapper med falske strekkoder med lavere pris enn den ordinære. Dette fører i sin tur til at det blir beregnet en lavere pris enn det som er korrekt. Strekkodene leses deretter automatisk inn i et datasystem hvoretter oppgjør skjer automatisk basert på uriktige priser uten mellomkomst av mennesker. Et annet eksempel er at et datasystem tilføres uriktig informasjon som pretenderer å være et gyldig kontonummer, i forbindelse med en helautomatisert bestillingsprosess. I begge tilfellene tilføres datasystemet uriktige opplysninger, jf. første alternativ i databedrageribestemmelsen. Utvalget foreslår derfor ikke § 270 første ledd nr. 2 opphevet.

Det antas at den ovennevnte løsning oppfyller forpliktelsen etter datakrimkonvensjonen artikkel 8.

### 5.8.7 «Tellerskrittsaker»

Såkalte «tellerskrittsaker» er en merkelapp på handlinger av nokså ulik karakter, men som har det til felles at de resulterer i en rettsstridig belastning av tellerskritt. Dette er en økonomisk vinning for gjerningspersonen. Man kan i det minste sortere disse handlingene i fire kategorier:

*Fysisk omkobling*

Det kan for eksempel være tale om omkobling av ledninger i en telefonsentral eller på telefonlinjen til naboen. Til illustrasjon kan det vises til saksforholdene i tellerskritt-dommene i Rt. 1989 side 980

og i Rt. 1992 side 790. Også den eldre metode «blue boxing» er i denne kategorien, dvs. at det kobles til et apparat til telefonen som simulerer langdistanse telefonsignaler, som utnyttes for gjerningspersonens eget telefonbehov. Denne metoden er gått ut av bruk etter at telefonsentralene ble digitalisert. Tapet påføres i det siste tilfellet telefonselskapet, mens i de andre er det avhengig av hvordan omkoblingen har skjedd. Tapet kan da enten falle på abonnenten eller direkte på telefonselskapet. Etter gjeldende rett anses dette som rettsstridig bruk av løsøregjenstand og er straffbart etter straffeloven §§ 261 og 393. Fremgangsmåtene vil kunne rammes av utkastet § 8, jf. alternativet som gjelder misbruk av elektronisk kommunikasjonsnett.

*Endring som skjer i datasystemet til telefonsentralen*

Her tenkes det på endring som foretas i datasystemet til telefonsentralen for å sørge for å kunne ringe uten at bruken blir registrert på en selv. Denne fremgangsmåte forutsetter regulært at gjerningspersonen også har skaffet seg uberettiget tilgang til datasystemet, noe som etter gjeldende rett rammes av straffeloven § 145 annet ledd. Etter rettsoppfatningen i pinkodekjennelsen i Rt. 1995 side 1872, ble endringene ansett som databedrageri. Etter lovforslaget vil slike handlinger være straffbare som ulovlig tilgang til datasystem, jf. utkastet § 4, og datamodifikasjon, jf. utkastet § 7.

*Misbruk av en annens telefonkort*

Misbruk av en annens telefonkort rammes i utgangspunktet som tyveri eller underslag (borttagelsen eller tilegnelsen av kortet er avgjørende), og lovforslaget gjør ingen endring i dette.

*Misbruk av en annens telefonabonnement*

Misbruk av en annens telefonabonnement oppnås for eksempel ved avgivelse av en pinkode. I så fall står man overfor et tilfelle av kontomisbruk, jf. utkastet § 16. Det samme gjelder ved bruk av såkalte «klonede» mobiltelefoner, en metode som ble benyttet på eldre mobiltelefoner (NMT-teknologi). Dette gikk ut på å benytte falsk abonnementsidentifikasjon som belastet bruken på andre lovlige abonnementer. Tilfellet kan sammenlignes med bruk av falske kredittkort som er fremstilt på grunnlag av skimming. Også dette er kontomisbruk, jf. utkastet § 16.

For de handlemåter som er regulert i lovforslaget er det adgang til å ta hensyn til vinningen og tapet i forbindelse med vurderingen av om lovbruddet er grovt, jf. utkastet § 18.

## 5.9 Elektronisk dokumentfalsk

### 5.9.1 Gjeldende rett

De viktigste reglene om dokumentfalsk finnes i dag i straffeloven §§ 179-186. Begrepet «dokument» er definert i § 179. Definisjonen gjelder både form og innhold. I innhold er et dokument en tilkjennegivelse som er av betydning som bevis for en rett, en forpliktelse eller en befrielse fra en forpliktelse eller som fremtrer som bestemt til å tjene som bevis. I form er et dokument en gjenstand som i skrift eller på annen måte har et slikt innhold som nevnt.

Reglene gjelder både helt falske og forfalskede dokumenter, men ikke uriktig innhold i ekte dokumenter. Straffeloven § 182 og § 183 er straffebud som retter seg mot bruken av et falsk eller forfalsket dokument. Straffeloven § 185 gjelder selve forfalskningen eller anskaffelsen av falsk dokument og § 186 gjelder forberedelse.

Det er uklart i hvilken utstrekning data og databasert informasjon skal regnes som dokument og faller inn under reglene om dokumentfalsk. I diskusjonen om dette har begrepet «elektronisk dokument» vært lansert. I den såkalte BBS-dommen i Rt. 1991 side 532, hvor de domfelte blant annet ble dømt for overtredelse av straffeloven § 183, bemerket Høyesterett:

> «Det er i og for seg klart at uberettigede endringer av data etter omstendighetene kan rammes som benyttelse av falsk dokument, jf. drøftelsen i NOU-1985-31 side 11-12.»

Når man i denne sammenheng anser data som en gjenstand, er det ved å anvende det funksjonelle gjenstandsbegrep, som er nærmere omtalt i kapittel 5.5.1. og 5.6.3.

For øvrig vises det til Andenæs og Bratholm: «Spesiell strafferett», 3. utg side 283-321, se særlig side 300, Sunde: «Elektronisk dokumentfalsk», Økokrims skriftserie nr. 9, 1995: «Datakriminalitet» side 202-210, NOU 1985: 31 side 11-12 og Schjølberg: «Cybercrime» side 60-64.

I motivene til nåværende straffelov er reglene om dokumentfalsk betegnet som en forbrytelse mot offentlig tillit (publica fides). Dette er tenkt videreført i ny straffelov, jf. NOU 2002: 4 side 374, hvor reglene foreslås videreført under kapitlet om «Vern av tilliten til dokumenter og penger». Dette innebærer at reglene kan anvendes i konkurrens med andre bestemmelser som verner andre goder, for eksempel datakrimbestemmelsene.

### 5.9.2 Datakrimkonvensjonen artikkel 7

Datakrimkonvensjonen artikkel 7 lyder slik i norsk oversettelse:

«Artikkel 7 - Datarelatert falsk

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbare handlinger etter nasjonal rett, forsettlig, urettmessig tilførsel, endring, sletting eller fjerning av elektroniske data som fører til ugyldige data, i den hensikt at de skal anses som eller brukes i rettslig sammenheng som om de var ekte, enten de er direkte lesbare og forståelige eller ikke. En part kan stille som vilkår at det må foreligge svikaktig eller annen uredelig hensikt før straffansvar pådras.»

I NOU 2003: 27 viste Datakrimutvalget til straffeloven § 182 sammenholdt med Rt. 1991 side 532, og konkluderte med at det ikke var nødvendig med endringer i norsk rett for å oppfylle konvensjonens krav.

### 5.9.3 Straffelovkommisjonens syn

I NOU 2002: 4 har Straffelovkommisjonen forelått at reglene om dokumentfalsk skal videreføres i kapittel 31 i ny straffelov i betydelig forenklet form. Kapitlet har overskriften «Vern av tilliten til dokumenter og penger». Kommisjonen går inn for at straffebudet først og fremst skal rette seg mot forfalskningen. Bare dersom den som bruker det falske dokumentet ikke kan straffes for forfalskningen eller anskaffelsen av dokumentet, forelås bruken gjort straffbar som selvstendig overtredelse.

Kommisjonen uttaler at det ikke er innlysende at begrepet «dokument» bør videreføres. Begrunnelsen for dette er at begrepet i dag også anvendes på bevismidler som er fjernt fra ordets betydning i alminnelig språkbruk, blant annet på elektronisk lagret informasjon.

### 5.9.4 Datakrimutvalgets syn

Det faller utenfor Datakrimutvalgets mandat å utrede nye regler om dokumentfalsk. Dette har imidlertid en side mot datakriminalitet som fordrer klargjøring: I hvilken utstrekning skal falske data bedømmes etter de samme regler som falske papirdokumenter. I denne forbindelse har Datakrimutvalget valgt å presentere en skisse til enkelte regler i dokumentfalskkapitlet. Mer enn en skisse er det imidlertid ikke tale om, siden utvalget bare går inn på enkelte sider ved reglene om dokumentfalsk.

I prinsippet foreligger det flere alternative løsninger. En løsning kan være å ta inn en egen paragraf i datakapitlet som er bygget på samme lest som datakrimkonvensjonen artikkel 7 og utelate elektronisk lagret informasjon fra kapitlet om dokumentfalsk. Dette kan imidlertid skape tvil om hvor enkelte varianter skal henføres, for eksempel epost og sms-meldinger.

En annen løsning er å regulere dette i kapitlet om dokumentfalsk som i dag. I så tilfelle er det nødvendig å foreta endringer i definisjonene som i dag finnes i straffeloven § 179 for å klargjøre det presise anvendelsesområdet for bestemmelsene.

Begrepsmessig foreligger det to mulige løsninger. Den ene er å foreta en abstraksjon og lansere et nytt begrep som trer istedetfor begrepet dokument. Det nye begrepet må være videre enn det gamle dokumentbegrepet. En mulig betegnelse på et slikt begrep er «bevisbærer». Alternative begreper er «bevismidler» eller «bevisrepresentasjoner». En annen løsning er å lansere en underkategori under begrepet «dokument», som kalles «elektronisk dokument». Datakrimutvalget har blitt stående ved at den første typen løsning vil være enklest. Betegnelsen «elektronisk dokument» vil nok i utgangspunktet ha en kjerne som er lett å knytte til begrepet, for eksempel epost, lagrede tekstfiler m.v., men vil i andre tilfeller virke anstrengt i forhold til det som er ment rammet, for eksempel innhold i databaser og datalogger. Det synes derfor unødvendig kompliserende å anvende begrepet «elektronisk dokument». Anvender man et samlebegrep, er det heller ikke nødvendig å ta stilling til i hvilken underkategori det enkelte tilfelle skal henføres.

### 5.9.5 Elektroniske sertifikater og signaturer

Elektroniske sertifikater og signaturer er omhandlet ovenfor i kapittel 3.2.5. Esignaturloven har straffebestemmelser i § 21. Disse reglene gjelder imidlertid leverandører som unnlater å oppfylle sine plikter etter loven. Straffebestemmelsene der tar ikke sikte på misbruk av elektroniske signaturer eller sertifikater.

I forarbeidene til esignaturloven (Ot.prp. nr. 82 (1999-2000)) uttales det i kapittel 3.5:

«Den tekniske utviklingen på området går raskt og en elektronisk signatur som er sikker i dag, er neppe like sikker mot forfalskninger om noen år. Det bør overveies hvorvidt dokumenter, hvor det er behov for å identifisere undertegneren på en sikker måte også etter at sertifikatets gyldighetstid har utløpt, egner seg for elektronisk kommunikasjon, f. eks. avtaler som gjelder over lang tid eller testament. [...] NTNU uttaler at man ikke bør bruke elektroniske signaturer på dokumenter som skal være gyldige i mer enn ti år, på grunn av risikoen for at tilbakedaterte dokumenter kan signeres og

dateres med et tidspunkt da signaturen var gyldig, dersom noen skulle klare å urettmessig tilegne seg signaturfremstillingsdataene.»

Det er på denne bakgrunn ingen tvil om at det er behov for å ta inn bestemmelser som rammer fremstilling av falske og forfalskede elektroniske signaturer og sertifikater i straffeloven. Utvalget har kommet til at det mest naturlige stedet å regulere slike tilfeller i straffeloven er i tilknytning til straffelovens regler om dokumentfalsk.

Et forhold påkaller særskilt oppmerksomhet: En vanlig underskrift vil alltid være falsk hvis den ikke er skrevet av rette vedkommende. En falsk elektronisk signatur kan imidlertid påføres av uvedkommende men likevel være ekte. Dette vil være tilfelle hvis signaturen påføres ved hjelp av tekniske hjelpemidler. Det er imidlertid åpenbart at dette bør være straffbart. Forutsetningen for dette er imidlertid at det er gjort uberettiget. Om sjefen for eksempel ber sekretæren påføre et elektronisk dokument sjefens elektroniske signatur, vil ikke dette være uberettiget. Forholdet skal da naturligvis heller ikke være straffbart.

Som nevnt inneholder esignaturloven og forskrift om krav til utsteder av kvalifiserte sertifikater m.v. straffebestemmelser. Disse straffebestemmelsene knytter seg til de strukturelle forholdene og beskytter selve PKI-strukturen. Datakrimutvalget ser derfor ingen grunn til å fremme noe forslag på dette området.

### 5.9.6 Datakrimutvalgets skisse til definisjonsparagraf

Datakrimutvalget foreslår følgende skisse til definisjonsparagraf:

«§ 31-1 Definisjoner
Med bevisbærer menes i dette kapitlet skriftlig dokument, trykt skrift, merke, data eller annet som etter sin art er beregnet på eller egnet til å tjene som bevis.

§ 31-2 Særregler for elektronisk signatur
Når elektronisk signatur er benyttet, anses objektet alltid som bevisbærer. Elektronisk signatur som uberettiget er påført av uvedkommende, regnes alltid som falsk bevisbærer.»

### 5.9.7 Kommentarer til forslaget

Ved utformingen av definisjonen av ordet «bevisbærer» er det sett hen til det tilsvarende begrepet «informasjonsbærer» i ny straffelov § 76. Forslaget inneholder som tidligere både definisjon av form og innhold.

Når det gjelder *innhold*, omfatter forslaget dispositive utsagn, erklæringer, logger og annet så fremt det er beregnet på eller egnet til å tjene som bevis. Hovedsakelig tenker en her på bevis som kan anvendes i rettslig sammenheng, men en har ikke funnet grunn til å avgrense til dette i lovteksten. En attest fra tidligere arbeidsgiver bør for eksempel falle inn under definisjonen uavhengig av om den er aktuell å benytte i rettslig sammenheng eller ikke. Bevisene kan gjelde både rettslige og faktiske forhold, men det er naturlig å holde utenfor det som gjelder rene faktiske forhold som er uten betydning i rettslig sammenheng. Utvalget finner ikke grunn til å gå nærmere inn på definisjonen av innholdet, da denne må vurderes uavhengig av formen. Det foreligger her ingen spesielle hensyn i forhold til teknologien.

For så vidt angår definisjonen av *formen*, vises det til definisjonen av begrepet «data» i datakrimkapitlet § 1. Enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk utstyr anses som data. Dette vil for eksempel omfatte informasjon som er lagret i magnetstripe eller en integrert krets på et kort. Definisjonen omfatter data som ved maskinlesing fremtrer skriftlig, visuelt eller auditivt som definert i ny straffelov § 76.

Forslaget innebærer at e-post, tekstmeldinger, websider og lignende anses som bevisbærer så fremt innholdet er av en slik art at det faller inn under definisjonen. Det samme gjelder andre former for elektroniske publikasjoner, for eksempel tekster beregnet på nedlasting og tekstfiler beregnet for lesing på datamaskin, PDA etc, herunder elektroniske bøker. Innholdet i skjemaer som overføres over internett, for eksempel bestillingsformularer som brukes i nettbutikker, er også inkludert i definisjonen av bevisbærer. Slike skjemaer inneholder ofte moderne former for dispositive utsagn, som ligger i kjerneområdet for det som vernes etter bestemmelsene i kapitlet om dokumentfalsk. En skriftlig bestilling eller en bestilling på e-post omfattes tilsvarende av reglene. Bekreftelser sendt over internett i form av pinkode, for eksempel bekreftelse av elektronisk selvangivelse eller lignende, omfattes også av definisjonen.

Et bankkort eller et kredittkort er fysisk manifestert ved et plastkort som inneholder en mikrochip, en magnetstripe eller begge deler. Om man vil kalle plastkortet for et dokument eller en gjenstand, kan bero på skjønn. Magnetfeltet eller mikrochipen vil være en elektronisk representasjon. I begge sammenhenger faller dette under begrepet «bevisbærer».

Også data som er lagret i en database faller inn under begrepet, dog avhengig av innholdet. Dette

vil for eksempel gjelde data som er lagret i en offisiell database i en forvaltningsetat over personer som er tilstått drosjebevilling, eller et elektronisk eksamensregister ved en skole eller et universitet.

Datalogger er typiske eksempler på representasjoner som er egnet til bruk som bevis blant annet i rettslig sammenheng, for eksempel som bevis for ulovlig tilgang til datasystem eller for nedlasting av seksualiserte skildringer av barn. Det er derfor viktig at forfalskning av datalogger faller inn under bestemmelsene om dokumentfalsk.

Følgende fysiske representasjoner, som normalt også har elektronisk innhold, er som regel maskinlesbare og vil være typiske bevisbærere:

- Kredittkort, debetkort og tilsvarende kort. Dette gjelder også de deler av kortet som inneholder magnetstripe, mikrochips, mikroprosessor eller liknende.
- Elektroniske reisekort (alle deler av kortet).
- Andre fysiske representasjoner som benyttes som betalingsmidler, for eksempel armbånd eller smartkort som registrerer elektroniske betalinger, elektroniske billetter og alle tenkelige former for tilsvarende funksjonalitet i fremtiden.
- Elektroniske adgangskort.
- Kodekort for betalings-tv.
- Maskinlesbare strekkoder for innlesing av vareidentitet og priser ved handel.
- Elektroniske ringekort.
- Elektroniske gavekort.
- Kodegenerator.

Elektroniske sertifikater vil være et typisk eksempel på data som er beregnet på å tjene som bevis, og faller inn under definisjonen i utkastet til § 31-1.

Når det gjelder elektronisk signaturer, er det føyd til en særregel i forslaget til § 31-2. Dette klargjør at filer som inneholder slike signaturer alltid skal anses som bevisbærere. Dessuten er det føyd til en regel om at filer som inneholder elektroniske signaturer som påføres av urette vedkommende alltid skal anses som falsk bevisbærer. Elektroniske signaturer er et system som skal sikre at man kan stole på at noe virkelig kommer fra den det utgir seg for, og bør derfor være strafferettslig beskyttet uavhengig av innhold.

Utvalget antar at datakrimkonvensjonen artikkel 7 vil være dekket med den skisserte lovbestemmelsen. Utvalget finner det klart at data som bare finnes i maskinlesbar form også omfattes av den foreslåtte bestemmelsen så fremt innholdet faller inn under lovens definisjon. Det er derfor ikke nødvendig å presisere dette i lovteksten av hensyn til artikkel 7.

Endringer av data vil kunne være straffbart både etter bestemmelsen om falsk bevisbærer og etter reglene om datamodifikasjon i utkastet § 7. Bestemmelsene tar sikte på ulike sider av det straffbare forholdet, og kan anvendes i konkurrens. Tilsvarende kan bestemmelsene om dokumentfalsk etter omstendighetene anvendes i konkurrens med utkastet § 15 om identitetstyveri.

## 5.10 Skyldkravet

Forsett er den vanlige skyldform etter straffeloven, jf. § 40, og dette vil også være hovedregelen for fremtiden, jf. ny straffelov § 21, som lyder:

«Straffelovgivningen rammer bare forsettlige lovbrudd med mindre annet er bestemt».

Datakrimutvalget har lagt dette til grunn for bestemmelsene i datakrimkapitlet. Utgangspunktet er således at det må foreligge forsett med hensyn til de enkelte vilkår i straffebudene for at skyldkravet skal være oppfylt. Hva som skal til for å konstatere forsett er angitt i ny straffelov § 22.

I visse typer lovbrudd hvor skadepotensialet er særlig stort, har imidlertid utvalget funnet behov for å foreslå at også grovt uaktsomme handlinger anses straffbare, jf. utkastet § 17. Dette gjelder lovbrudd som beskrevet i utkastet §§ 7, 9, 10, 12 annet ledd og 13. Det er nærmere redegjort for overveielsene knyttet til grov uaktsomhet for de nevnte lovbrudd i kapittel 6.1 og 9.17.

Tre av straffebudene i datakrimkapitlet stiller spesielle krav til det subjektive: Dette er:

- Utkastet § 2, hvor det kreves at den elektroniske kartleggingen må skje «for å kartlegge sårbarheter».
- Utkastet § 3, hvor det kreves at den ulovlige anbringelsen skjer for å begå handlinger som nevnt i § 3 første ledd bokstav a og b.
- Ukastet § 16, hvor det kreves at kontomisbruket skjer «med forsett om vinning».

## 5.11 Medvirkningsansvaret

Den nye straffeloven § 15 bestemmer at medvirkning er straffbart med mindre annet følger av det enkelte straffebud. Utvalget har ikke funnet grunn til å foreslå noe unntak fra medvirkningsansvaret i straffebudene i lovforslaget. Straff for medvirkning forutsetter at medvirkeren oppfyller alle straffebetingelsene selvstendig sett. For så vidt gjelder skyldform betyr det at medvirkning må skje forsettlig, jf. ny straffelov § 21, med mindre det er tilstrekkelig med grov uaktsomhet, jf. utkastet § 17.

Ved datakriminalitet er det av interesse å belyse medvirkningsreglene for noen grupper av aktører som peker seg ut som særlig sentrale. Problemstillingene gir ikke foranledning til å foreslå konkrete lovtiltak, men de peker på områder hvor det er grunn til å forvente en vesentlig rettslig utvikling som myndighetene dermed bør rette oppmerksomheten mot. De grupper aktører som utvalget særlig har tenkt på er tjenesteytere, betalingsformidlere og utviklere og leverandører av dataprogrammer.

### 5.11.1 Tjenesteyterne

Tjenesteytere av informasjonssamfunnstjenester som definert i ehandelsloven § 1 annet ledd bokstav a og b, kan deles i to grupper i forhold til medvirkningsreglene. De tilbyderne som omfattes av ehandelsloven § 3 bokstav a, jf. § 1 annet ledd bokstav b, er tilbydere av «tjenester som består i å gi tilgang til, eller å overføre informasjon over, et elektronisk kommunikasjonsnett, eller i å være nettvert for data som leveres av tjenestemottakeren». For slike tjenesteytere er det etablert regler som griper inn i det alminnelige strafferettslige medvirkningsansvaret, jf. ehandelsloven §§ 15-18.

For tjenesteytere av andre informasjonssamfunnstjenester enn de ovenfor nevnte, jf. ehandelsloven § 3 bokstav a, jf. § 1 annet ledd bokstav a, gjelder det ikke slike ansvarsfrihetsregler, så for disse gjelder i utgangspunktet de ordinære regler om strafferettslig medvirkningsansvar.

Ansvarsfrihetsreglene etter ehandelsloven §§ 16 og 17 gjelder for tilbydere av tilgang og ren videreformidling. For handlinger som består i slik tjenesteyting skal det mye til for at det skal bli tale om noe strafferettslig medvirkningsansvar.

Ansvarsfrihetsregelen i ehandelsloven § 18 som gjelder for nettverter, antas å kunne få større betydning. Det vesentligste er vilkåret om at medvirkningsansvar bare kan gjøres gjeldende dersom det foreligger forsett. Straff for medvirkning som skjer uaktsomt – eller som i lovforslaget – grovt uaktsomt, kan ikke gjøres gjeldende overfor nettverten *qua* nettvert. Det betyr at de lovbrudd som er straffbare også ved grov uaktsomhet, jf. utkastet § 18, ikke kan anvendes overfor nettverten i rollen som nettvert. Dette gjelder utkastet §§ 7, 9, 10, 12 annet ledd og § 13. For nettverten som hovedmann gjelder det ingen ansvarsbegrensning.

Det kan reises spørsmål ved medvirkningsansvaret for tilbydere av pekere til andre nettsteder, herunder tilbydere av søketjenester, når pekeren eller søket retter seg mot nettsteder med straffbart innhold. I den såkalte Napsterdommen, Rt. 2005 side 41, ble eieren av et norsk nettsted dømt til å betale erstatning til en gruppe plateselskaper og artister, jf. åndsverkloven § 55, for å ha medvirket til å ha tilgjengeliggjort musikkfiler via internett i strid med opphavsmannens enerett. Nettstedet hadde lagt lenker til musikkfiler på andre nettsteder hvor musikken var opplastet uten rettighetshavernes samtykke. Høyesterett fant at medvirkningshandlingene fra saksøkte var forsettlige og meget klanderverdige.

Det antas at et strafferettslig ansvar må bedømmes på samme måte etter åndsverkloven § 54 – også etter de lovendringer som er gjort etter at forholdene som er omhandlet i dommen fant sted. Det antas videre at resultatet blir det samme også utenfor åndsverklovens område der det er bestemmelser om straffansvar for medvirkning. «Tilgjengeliggjøring» er imidlertid et vidt begrep som forholdsvis lett lar seg knytte opp til en medvirkende handling. Rekkevidden av medvirkningsansvaret kan være annerledes ved andre regler eller straffebud som anvender snevrere formuleringer. Utvalget har ikke hatt tilstrekkelig tid til å kunne utrede dette problemfeltet.

Det kan også være tvilsomt hvilken status tilbydere av søkemotor har i forhold til reglene i ehandelsloven, både om de er en tjenesteyter av en informasjonssamfunnstjeneste, og i så fall hvilket alternativ i ehandelsloven § 1 annet ledd bokstav a og b, som gjelder. Dette er avgjørende i forhold til reglene om ansvarfrihet. Hvis søkemotoren ikke regnes som en informasjonssamfunnstjeneste etter § 1 annet ledd bokstav b, gjelder ikke ansvarsfrihetsreglene, og det er dermed aktuelt å anvende de alminnelige medvirkningsreglene også for uaktsomme handlinger, når dette er en relevant skyldform etter straffebudet. Det er blant annet tilfelle både for overtredelse av reglene i åndsverkloven og reglene om spredning av seksualiserte skildringer av barn, jf. åndsverkloven § 54 og straffeloven § 204a. Utvalget nøyer seg her bare med å peke på problemstillingene uten å ta stilling til rettstilstanden de lege lata.

### 5.11.2 Betalingsformidlere

For så vidt gjelder betalingsformidleres mulige strafferettslige medvirkningsansvar, så er også dette et lite utredet område. Utvalget er ikke kjent med at det finnes ansvarsfrihetsregler for denne gruppen lik de som gjelder for tjenesteyterne. Det anses heller ikke som tvilsomt at betalingsformidlere kan holdes strafferettslig ansvarlig for medvirkning til ulovlig virksomhet dersom de vitende om virksomheten stiller sine tjenester til rådighet.

I mange tilfeller er oppgjørsmekanismen instrumentell for at det kan skje en lovovertredelse, for eksempel ved salg av seksualiserte skildringer av barn på internett. I så fall foreligger også utvilsomt medvirkning, dersom de subjektive vilkår er oppfylt. I praksis oppstår problemer med strafforfølgning fordi betalingsformidlingsbransjen opererer internasjonalt og det er lett å innrette seg slik at tjenestene ytes til brukersteder i land hvor risikoen for rettsforfølgning er liten.

En effektivisering av bekjempelse av den profittmotiverte internettkriminaliteten antas å kalle på flere tiltak, for eksempel ved å lempe på skyldkravet for betalingsformidlere (uaktsomhet som skyldform ved flere overtredelser) og økt kontrollplikt (noe som korresponderer med et strengere aktsomhetskrav). Det kan for øvrig også vises til at Justiskomiteen i Stortinget har vært opptatt av betalingsformidleres mulige strafferettslige ansvar. Særlig med tanke på å demme opp for seksuelt misbruk av barn har komiteen bedt regjeringen om å utrede mulighetene for å stoppe bruk av kredittkort på nettsteder som tilbyr seksualiserte skildringer av barn. Det vises til Innst. O. nr.66 (2004-2005) kapittel 2. Det kan videre vises til lignende betraktninger hos Goldsmith og Wu 2006 side 65-85. Ytterligere kan det vises til Sunde 2006 «Lov og rett i cyberspace» kapittel 8.2, 8.6 og 8.7 om medvirkningsspørsmål for tjenesteytere og betalingsformidlere.

### 5.11.3 Programutviklere og leverandører

Programutviklere og leverandører av slike programmer står selvsagt i en helt sentral rolle for utviklingen i det elektroniske miljøet, og det er av største betydning at programmene holder god kvalitet. En programmerer kan for eksempel forsettlig legge inn sårbarheter i et operativsystem som skaper sårbarhet i alle de maskiner som tar det i bruk. I slike tilfeller kan han rammes etter bestemmelsen om datamodifikasjon, jf. utkastet § 7, og eventuelt grov økonomisk utroskap overfor arbeidsgiver, jf. straffeloven §§ 275, jf. 276. Et annet spørsmål er om han kan rammes for medvirkning til den inntrengning som skjer når sårbarheten oppdages og utnyttes, dvs. medvirkning til overtredelse av utkastet § 4. Ulovlig tilgang er jo en påregnelig følge av handlingen, men det antas at det også må stilles visse krav til tidens, stedets og forsettets enhet, dvs. til adekvans. Dersom programmereren implementerer sårbarheten i forståelse med den som senere skal misbruke den, kan han straffes for medvirkning. Men han kan neppe straffes for medvirkning til det senere generelle misbruket.

Programmereren kan også benytte sin kompetanse til å skape skadelig kode. Dette rammes som en selvstendig straffbar handling, jf. fremstillingsalternativet i utkastet §§ 11 og 12. Vedkommende vil også kunne straffes for å ha spredt og ha markedsført den skadelige koden, jf. tilgjengeliggjøringsalternativet i de nevnte bestemmelsene og markedsføringsalternativet i § 11. Hvorvidt han i tillegg kan straffes for andres utnyttelse av programmet til straffbart bruk, må løses etter de ovenfor nevnte retningslinjer. Det er neppe rimelig å anvende medvirkningsansvar for den generelle bruk, i lys av at handlingen allerede kan straffes som et selvstendig straffbart forhold.

## 5.12 Rettighetstap, inndragning og vilkår for betingede dommer

Rettighetstap og inndragning er reaksjoner som ilegges i forhold til en lovbryter ved dom. Det kan derfor gå lang tid fra et lovbrudd blir begått til en slik reaksjon kan iverksettes. I mellomtiden er det mulig å anvende straffeprosessuelle tvangsmidler. Utvalget går imidlertid ikke nærmere inn på dette, da det faller utenfor utvalgets mandat.

### 5.12.1 Rettighetstap

Ny straffelov § 56 gjelder rettighetstap. Etter § 56 vil den som har begått en straffbar handling som viser at vedkommende er uskikket til å utøve en aktivitet, kunne fradømmes retten til for fremtiden å utøve denne aktivitet. Dette kan bare skje når allmenne hensyn tilsier det. Bestemmelsen er en kan-bestemmelse, som gir domstolen rom for skjønn. Ved et slikt skjønn, antas det at domstolen må foreta en vurdering av om reaksjonen står i et rimelig forhold til den straffbare handlingen som er begått.

Etter annet ledd må det antas at rettighetstapet kan begrenses til forbud mot visse deler av aktiviteten. Det kan også gis påbud om å utøve aktiviteten på bestemte vilkår.

Rettighetstap kan ilegges som eneste straff hvis det ikke er fastsatt en minstestraff på fengsel i ett år eller mer for handlingen. Det følger av § 58 at rettighetstap ilegges for en bestemt tid, maksimalt inntil 5 år.

Det synes klart at aktuelle eksempler på rettighetstap etter denne bestemmelsen er fradømmelse av retten til å bruke datamaskin og fradømmelse av retten til å bruke internett. Rettighetstapet kan også begrenses til for eksempel forbud mot å bruke chattekanaler på internett; se Ot.prp. nr. 90 (2003-2004) side 454.

Et individualpreventivt tiltak kan for eksempel være å forby personer som er domfelt for hacking adgang til internett for en periode.

Datakrimutvalget bemerker at reaksjoner av denne typen av og til kan være hensiktsmessige i datakrimsaker. Vedtatte lovhjemler er her tilstrekkelige, og utvalget finner ikke grunn til å fremme forslag om nye bestemmelser på dette punktet. Denne typen reaksjon er aktuell ikke bare ved den rene datakriminalitet, men ved all kriminalitet hvor datautstyr har vært benyttet som middel for å begå kriminaliteten, for eksempel ved befatning med seksualiserte skildringer av barn.

Reaksjoner av denne typen er vel kjent fra utlandet. Det vises til Smith, Grabosky og Urbas: «Cyber Criminals on Trial», Cambridge University Press (Australia) 2004 side 119-120 samt side 182, 197, 198, 205, 212, 219 og 223. I USA har det i slike saker vært flere anker som har vært begrunnet med at totalforbud mot bruk av datamaskiner eller totalforbud mot bruk av internett har vært en for omfattende reaksjon. I enkelte tilfeller har anke på dette grunnlag ført frem, og overordnet domstol har fastsatt mindre inngripende restriksjoner.

Det har også vært fastsatt vilkår om monitoring (overvåking) av datamaskin- eller internettbruk. Slike vilkår synes forenelig med ny straffelov § 56 annet ledd.

Problemene som knytter seg til denne typen restriksjoner er for det første kontroll. Det er vanskelig å kontrollere om domfelte innretter seg i samsvar med det idømte rettighetstapet. Det vil alltid være muligheter til å låne en datamaskin, benytte en internettkafé osv. Dette gjør at tiltak av denne typen lett kan bli et slag i luften.

For enkelte typer rettighetstap, for eksempel totalforbud mot bruk av internett, vil også vedkommende få vanskeligheter blant annet med kommunikasjon med offentlige myndigheter, som ønsker mest mulig elektronisk kommunikasjon med borgerne. Domfelte vil også kunne bli utestengt fra å handle på nettet og foreta lovlige transaksjoner som er mulig for alle andre. Slike forhold må imidlertid, etter utvalgets oppfatning, bli en del av domstolenes konkrete vurdering i den enkelte sak.

### 5.12.2 Inndragning av redskapet til en straffbar handling

Ny straffelov § 69 gir hjemmel for å inndra «ting» som har vært brukt eller er bestemt til bruk ved en straffbar handling. Det følger av annet ledd at som «ting» regnes også bl.a. elektronisk lagret informasjon.

Det er etter dette klart at datautstyr som har vært benyttet til å begå en straffbar handling kan inndras. For eksempel kan en inndra en datamaskin hos en person som har skaffet seg ulovlig tilgang til et datasystem, eller hos en som dømmes for befatning med seksualiserte skildringer av barn over internett. Andre eksempler på fysiske ting som kan inndras vil være tastetrykksregistrator (key stroke logger) og libanesisk slynge (Lebanese loop). Disse begrepene er det gjort nærmere rede for i kapittel 5.4.3 og 3.5.4.

Også elektronisk lagret informasjon regnes altså som ting. Dette vil for eksempel kunne gjelde en liste over kredittkortnumre som har vært brukt eller kan brukes i forbindelse med databedrageri. Et annet eksempel er en liste over passord som har vært brukt til eller kan brukes til å skaffe seg ulovlig adgang til andres datasystemer.

Også dataprogrammer kan være redskaper for å begå straffbare handlinger. Et eksempel på slike programmer er såkalte exploits, som er programmer beregnet på å utnytte sårbarheter i datasystemer og som kan muliggjøre ulovlig inntrengning. Spørsmålet er om dataprogrammer omfattes av begrepet «elektronisk lagret informasjon». For å gjøre dette utvilsomt, foreslår Datakrimutvalget at § 69 annet ledd endres til å lyde slik:

> «Som ting regnes også rettigheter, fordringer og elektronisk lagret informasjon, *herunder dataprogrammer.*»

Siden elektronisk informasjon ikke er en fysisk gjenstand, oppstår spørsmålet om hvordan inndragning skal gjennomføres. Dette kan enten skje ved at det fysiske mediet de er lagret på (for eksempel harddisken i en datamaskin) blir inndratt, eller ved at informasjonen slettes. En sikker sletting er imidlertid ikke lett å gjennomføre, så den første måten er å anbefale. Dette kan gjennomføres ved at domstolen i inndragningsdommen, eventuelt politiet i inndragningsforelegget, gir anvisning på at både det konkrete lagringsmediet og dets innhold skal inndras. Inneholder lagringsmediet også elektronisk informasjon som ikke er gjenstand for inndragning, bør domfelte kunne få en kopi av denne informasjonen for videre bruk.

Bestemmelsen suppleres med straffeloven § 76, som gir særregler for inndragning av informasjonsbærere. Bestemmelsen er ikke en selvstendig inndragningshjemmel. Det fremgår klart av forarbeidene (Ot.prp. nr. 90 (2003-2004) side 465) at for eksempel harddisker og cd-er er å anse som informasjonsbærere.

Det følger av den nye straffeloven § 76 annet ledd at den som må tåle inndragningen kan kreve

informasjonsbæreren tilbakelevert etter at det ulovlige innholdet er fjernet. Vedkommende må i tilfelle dekke utgiftene. Hvis inndragningen gjelder data, er det, som det fremgår ovenfor, ikke tilstrekkelig å slette det ulovlige innholdet. Dette kan lett gjenopprettes av kyndige personer etter en vanlig sletting. I slike tilfeller må politiet i tilfelle benytte spesialutviklede programmer for å foreta en effektiv sletting. En enklere fremgangsmåte, som neppe kan være i strid med loven, er at domfelte mot å dekke utgiftene får en kopi av det lovlige innholdet som fantes på lagringsmediet slik det er nevnt ovenfor.

Det foreslås derfor at § 76 annet ledd endres slik:

> «Ved inndragning av informasjonsbærer skal det angis hvilke deler av innholdet som begrunner inndragning. Den som må tåle inndragningen, kan mot å dekke utgiftene kreve informasjonsbæreren tilbakelevert etter at det ulovlige innholdet er fjernet. *Gjelder inndragningen data, kan påtalemyndigheten likevel mot at den som må tåle inndragningen dekker utgiftene, istedenfor å tilbakelevere informasjonsbæreren, gi vedkommende en kopi av de data som fantes på informasjonsbæreren og som ikke omfattes av inndragningen.*»

Det følger av den nye straffeloven § 71 at inndragning etter § 69 skal foretas overfor lovbryteren. Kreves det inndragning av ting som ikke tilhører lovbryteren, reises kravet mot eieren, jf. ny straffelov § 74 første ledd. Et eksempel på dette er at datautstyr inndras fra foreldrene selv om det er barna som har benyttet det til straffbare handlinger. Ny straffelov § 74 annet ledd åpner for at inndragning kan skje overfor besitteren dersom eieren eller rettighetshaveren er ukjent eller ikke har kjent oppholdssted i Norge. Om verken lovbryteren eller besitteren har kjent oppholdssted i Norge, kan inndragning skje uten at noen gjøres til saksøkt, jf. § 74 tredje ledd.

Inndragning etter disse bestemmelsene kan ha varierende effekt. Inndras det en datamaskin, vil lovbryteren lett kunne anskaffe eller låne en ny. Dette blir imidlertid ikke annerledes enn i andre tilfeller av inndragning, for eksempel av innbruddsverktøy.

### 5.12.3 Stengning av nettsteder, konto hos tjenesteyter m.v.

Det synes klart at et nettsted kan stenges etter bestemmelsene i straffeloven § 69. Et nettsted er representert ved elektronisk lagret informasjon, og kan inndras hvis det har vært brukt eller er bestemt til bruk ved en straffbar handling. Eksempler på slike er nettsider som inneholder seksualiserte skildringer av barn eller hvor det foregår fildeling med mulighet til for eksempel ulovlig nedlasting av musikk m.v. Også et nettsted som er opprettet for å begå bedrageri i forhold til kundene kan inndras etter denne bestemmelsen. Et typisk eksempel på dette er en såkalt phishing-nettside, se kapittel 3.5.12. På dette området suppleres § 69 av § 76, som er en særregel om inndragning av informasjonsbærere. Det er klart at en webserver er en informasjonsbærer etter definisjonen i første ledd. § 76 er nærmere omtalt ovenfor.

I de fleste tilfeller eier ikke den som er innehaver av nettsidene webserveren selv. Vedkommende har isteden konto hos en tjenesteyter. Stengning av nettstedet må da kunne skje ved at leverandøren (tjenesteyteren) pålegges å stenge nettstedet istedenfor at man inndrar nettleverandørens (ISP-ens) server. Det vil her være tale om å stenge en konto og krever ikke inndragning av hele serveren. Dette fremgår imidlertid ikke klart av loven.

Ehandelsloven inneholder regler som i en viss utstrekning garanterer straffrihet for en tjenesteyter, herunder en isp (internet service provider), jf. ehandelsloven § 16. Inndragning er ikke straff, men en strafferettslig reaksjon. Etter utvalgets oppfatning vil da ikke ehandelsloven være til hinder for at inndragning i visse tilfeller kan ha en tjenesteyter som prosessuell motpart. I alle fall presiserer ehandelsloven § 20 at bestemmelsene i ehandelsloven ikke er til hinder for at en domstol krever at tjenesteyteren bringer en overtredelse til opphør eller hindrer den.

I tilnytning til ny straffelov § 71, jf. også § 74, kan det oppstå noen spørsmål om hvem som skal gjøres til motpart i sak om inndragning i disse tilfellene. For å klargjøre dette i de tilfellene hvor eieren av nettsidene benytter seg av en konto hos en tjenesteyter for å publisere nettsidene sine, fremmer utvalget forslag om en ny § 76a i straffeloven. Denne paragrafen gjelder imidlertid ikke bare webservere, men også andre tilfeller hvor det benyttes konto hos andre (tjenesteyter) for datadrift og/eller oppbevaring av data. Blant annet gjelder det når adgang til internett kjøpes gjennom en tjenesteyter.

En datamaskin kan benyttes for fildeling på peer-to-peer basis. Dette innebærer at to eller flere datamaskiner koblet til internett kan dele filer. Et nettverk for fildeling mellom datamaskinene kan etableres ved at man benytter dertil egnet programvare. Har man for eksempel ulovlig delt musikkfiler på denne måten, vil de involverte data-

maskinene kunne inndras. I slike tilfeller kunne det være et alternativ å stenge gjerningspersonenes internettforbindelse ved pålegg til tilbyderen av internettilgangen. § 76 inneholder ikke hjemmel for dette, men her kan man gå frem etter bestemmelsene om rettighetstap, som er omtalt ovenfor. Datakrimutvalgets forslag til ny § 76a vil også åpne for denne muligheten. Forskjellen mellom denne fremgangsmåten og rettighetstap, vil være at rettighetstap også vil hindre at domfelte oppretter en ny konto hos en annen tilbyder. De to tiltakene kan eventuelt kombineres.

Det kan også i andre tilfeller være aktuelt å foreta inndragning ved å stenge en konto. Dette kan for eksempel være en konto på en side som viser bilder til medlemmer, tillater medlemmer å opprette en blogg, lukkede chattekanaler m.v. Det kan også være tale om å inndra rettighetene til å benytte ip-telefoni eller adgangen til å benytte ulike direkte kommunikasjonskanaler.

For å klargjøre dette, foreslår utvalget en ny § 76a, som kan lyde slik:

> «§ 76a Særregler for inndragning av konto på datasystem.
>
> Ved inndragning av en konto på et datasystem kan tjenesteyteren pålegges å stenge domfeltes tilgang til datasystemet og å slette innhold som tilhører domfelte.
>
> Inndragning etter første ledd foretas overfor rettighetshaveren til kontoen. Er vedkommende ukjent eller ikke har kjent oppholdssted i Norge, foretas inndragning overfor tjenesteyteren eller besitter av datasystemet såfremt det finnes rimelig av hensyn til rettighetshaveren til kontoen. Inndragning kan foretas overfor andre enn rettighetshaveren til kontoen selv om vedkommende var i god tro. Rettighetshaveren til kontoen skal så vidt mulig gis varsel om saken. Er verken rettighetshaveren til kontoen eller tjenesteyteren kjent eller har oppholdssted i Norge, kan tingretten beslutte inndragning på de vilkår som er nevnt i annet punktum uten at noen er gjort til saksøkt.»

Reglene i bestemmelsen er så godt som mulig harmonisert med reglene i § 74. En konto kan ha vært benyttet av andre enn den som er rettighetshaver til kontoen. Utvalget ser det ikke som nødvendig å komplisere reglene med at også en slik person må gjøres til part i inndragningssak. Inndragning etter denne bestemmelsen er ment å kunne gjennomføres i forhold til tjenesteyter selv om tjenesteyter ikke kan klandres for det straffbare forholdet. Dette er klargjort i annet ledd tredje punktum. Dette synes nødvendig av hensyn til bestemmelsene i ny straffelov § 71 tredje ledd sammenholdt med § 69 første ledd bokstav c. Begrepet «tjenesteyter» er benyttet på samme måte som i ehandelsloven, jf. definisjonen i ehandelsloven § 3 bokstav a.

Ny straffelov § 70 gjelder forebyggende inndragning. Første ledd tredje punktum begrenser denne regelens rekkevidde i forhold til informasjonsbærere. Informasjonsbærere kan bare inndras etter denne bestemmelsen når det er fare for uopprettelig skade. Datakrimutvalget ser ingen innvendinger mot å opprettholde denne begrensningen ved forebyggende inndragning.

I en avgjørelse fra dansk Højesteret (sak 49/2005) ble en internettilbyder pålagt å stanse overføringen fra to internettservere som tilgjengeliggjorde et stort antall musikkfiler. Det var ikke kjent hvem som eide serverne. Internettilbyder anførte at forbudet i realiteten medførte at abonnentenes internettforbindelse måtte stenges, og at et slikt forbud ville være et uforholdsmessig inngrep. Højesterett la imidlertid til grunn at innehaverne av serverne hadde foretatt omfattende krenkelser av opphavsrettigheter til musikkverker, og at også internettilbyderen hadde foretatt handlinger som stred mot rettighetshavernes rettigheter, og nedla forbud overfor internettilbyderen mot å overføre slikt innhold fra de nevnte servere. Højesteret fant at det ikke var grunnlag for å fastslå at forbudet ville medføre skade eller ulempe som sto i åpenbart misforhold til rettighetshavernes interesse i nedleggelse av forbudet.

Også ved inndragning etter norske regler skal det foretas en forholdsmessighetsvurdering, jf. ny straffelov § 69 tredje ledd.

### 5.12.4 Vilkår for betingede dommer

Bestemmelsene om vilkår for dommer på betinget fengsel finnes i ny straffelov § 34 sammenholdt med §§ 35-38. Etter § 37 bokstav j kan retten som særvilkår for fullbyrdingsutsettelse pålegge den domfelte å oppfylle særvilkår som retten finner hensiktsmessig. Det fremgår av Ot.prp. nr. 90 (2003-2004) side 439 at slike vilkår må ha som formål å fremme den domfeltes resosialisering eller bidra til å bøte på skaden ved den straffbare handling.

Datakrimutvalget antar at det for eksempel kan settes som vilkår at domfelte for en periode ikke skal benytte internett eller være underkastet restriksjoner om begrenset bruk av internett.

Vilkår av denne art kan således fastsettes både i medhold av straffeloven § 56 og § 37. Fordelen med å benytte § 37 vil være at bruk av datautstyr i strid med vilkårene vil representere brudd på vil-

kårene og sanksjoneres overensstemmende med dette.

I utlandet har en benyttet blant annet vilkår om overvåking av domfeltes datamaskinaktivitet og uanmeldte inspeksjoner av datautstyr. Det vises til Smith, Grabosky og Urbas: «Cyber Criminals on Trial» side 121.

Datakrimutvalget finner at bestemmelsen i den form den er vedtatt gir hjemmel for relevante strafferettslige reaksjoner i forbindelse med datakriminalitet, og finner det ikke nødvendig å foreslå endringer på dette punkt. Det presiseres at effekten av slike vilkår kan være begrenset, i og med at det kan være vanskelig å føre effektiv kontroll med om vilkårene overholdes. De øvrige motforestillinger som er beskrevet ovenfor både i forhold til rettighetstap og inndragning, gjelder også ved vilkår i betingede dommer. Det er likevel slett ikke utelukket at slike vilkår kan være hensiktsmessige i enkelte saker.

## 5.13 Filtrering

### 5.13.1 Problemstilling

Problemstillingen gjelder filtrering av utenlandske nettsteder som tilgjengeliggjør informasjon som er ulovlig etter norske regler. Her kan ikke reglene om inndragning anvendes. Filtrering går ut på å iverksette tiltak som hindrer at norske tjenestemottakere kan motta slik informasjon eller utnytte ulovlige tjenester. Informasjonen eller virksomheten kan bli distribuert fra jurisdiksjoner som har andre regler enn Norge, for eksempel såkalte «data havens» eller land som det i praksis er vanskelig å samarbeide med og som mangler myndigheter som håndhever reglene effektivt. Det kan også være land som har andre materielle strafferegler enn Norge. For eksempel er spill om penger (for eksempel poker) i utgangspunktet både forbudt og uønsket i Norge, mens det er fullt legalt og vanlig i mange andre land. Spørsmålet er om filtrering bør tas i bruk som et ensidig nasjonalt tiltak for å hindre norske borgere i å motta slik utenlandsk informasjon eller tjenester, som er straffbart etter norske regler. Filtrering vil gi samme effekt for norske tjenestemottakere på internett, som når en server eller et nettsted inndras slik at den ikke lenger kan tilgjengeliggjøre den ulovlige informasjon.

Utvalget har her delt seg, slik at kun et mindretall går inn for å foreslå filtrering. I det følgende gis først en beskrivelse av hva man tenker på som filtrering.

### 5.13.2 Filtreringsmetoder

Filtrering kan skje på nasjonalt nivå eller på tilbydernivå.

Et land som bruker filtrering på nasjonalt nivå er Kina. På denne måten har kinesiske myndigheter skaffet seg kontroll over innbyggernes bruk av internett. Norge har ikke infrastruktur som muliggjør filtrering på nasjonalt nivå og det antas heller ikke å være aktuelt å bygge ut en slik omfattende mulighet.

Filtrering kan også skje på tilbydernivå; gjennom de enkelte internettleverandørene. Dette gjøres i Norge gjennom filtre som fanger opp sider inneholdende seksualiserte skildringer av barn. I stedet for å få opp kjente nettsteder med denne typen innhold, får man ved surfing fra Norge opp en plakat fra Kripos som forteller at nettstedet er blokkert og at bruk av nettstedet vil være straffbar. Ordningen er innført ved et samarbeid mellom norske myndigheter og internettleverandørene. Ordningen er frivillig, og de fleste internettleverandørene deltar. Så vidt utvalget kjenner til, deltar ikke alle internettleverandørene i dette samarbeidet, og filtreringsordningen er derfor bare delvis effektiv. I forbindelse med at Stortinget behandlet forslaget til ny lovbestemmelse om seksualiserte skildringer av barn, uttalte Justiskomiteen i Innst. O. nr. 66 (2004-2005):

> «Komiteen har merket seg at Telenor som internettilbyder har utviklet et filter for å stenge tilgang til nettsteder som inneholder fremstillinger av seksuelle overgrep mot barn og/eller fremstillinger som seksualiserer barn. Dette filteret er utviklet etter initiativ fra justisminister Odd Einar Dørum, og i samarbeid med KRIPOS og Redd Barna. Filteret stopper nettsider som KRIPOS anbefaler at skal filtreres bort. Nettsteder som innholder materiale som nevnt bidrar for det første til å gjøre barnepornografisk materiale tilgjengelig for interesserte, og bidrar slik til nyrekruttering til dette markedet. For det andre er disse nettstedene inngangsportaler til mer alvorlig barnepornografisk materiale, og bidrar på denne måten til spredning av dette.
>
> Komiteen er klar over at et filter som ovenfor nevnt kun vil stenge tilgang til nettstedene, og ikke vesentlig bidra til å begrense spredning av barnepornografisk materiale gjennom andre kanaler. Komiteen mener likevel at det vil ha en begrensende virkning på tilgangen, spesielt for nye interesserte.
>
> Komiteen mener at alle internettilbydere i Norge bør ha et slikt filter, og ber Regjeringen påvirke bransjen for å oppnå dette. Det bør etter komiteens mening etableres en ordning

med felles oversikt over nettsteder som det skal nektes tilgang til. Ansvaret for en slik ordning bør tillegges egnet nivå hos justismyndighetene i samarbeid med internettilbyderne. Komiteen ber Regjeringen følge utviklingen i bransjen nøye. Dersom ikke internettilbyderne i Norge har et filter som nevnt innen utgangen av 2006, ber komiteen Regjeringen fremme forslag for Stortinget som påbyr dette.»

Filtering har svakheter ved at det verken er fullstendig effektivt eller treffsikkert. Filtreringstiltak kan omgås og det kan også finnes tjenesteytere som ikke gjennomfører filtrering. Dette vil være tilfelle enten en slik ordning er avtalebasert eller lovpålagt. Videre kan det være et problem at filtrering blokkerer materiale som ikke er ment å blokkeres («falske positiver»). Problemet er vanskelig å unngå fordi filtrering skjer mot den datamaskin (målvert) som sender materialet og ikke direkte mot det ulovlige materialet. Dersom maskinen også sender lovlig materiale, blokkeres også dette. Til tross for svakhetene kan det hevdes at filtrering er et egnet virkemiddel fordi det tross alt kan stanse en viss andel av den ulovlige trafikken. Hvor stor andel som stanses er det likevel vanskelig å ha noen sikker formening om, i hvert fall uten å ta i bruk store ressurser for å kartlegge tjenestemottakernes nettbruk.

### 5.13.3 Flertallets syn

*Flertallet, Gulbrandsen, Sellæg, Taraldset og Willassen* finner ikke grunn til å foreslå en slik lovhjemmel. Flertallet mener at hensynet til ytringsfriheten taler mot å sensurere utenlandske nettsider for norske brukere. EMK artikkel 10 beskytter i utgangspunktet alle typer ytringer, uansett form og innhold.

Det faktum at bruk av de eksisterende filtreringsmetoder, innholdskontroll ved søketermer og blokkering av bestemte målverter, samtidig innebærer en stor mulighet for såkalte «falske positive», det vil si at også legitim trafikk stoppes av filteret, tilsier at hensynet til ytringsfriheten bør veie tungt i denne sammenheng. Risikoen for falske positive er særlig et problem ved blokkering av bestemte målverter fordi det er vanlig at innhold fra mange forskjellige aktører er samlet på samme server som tilhører én tjenesteyter. Flertallet legger stor vekt på at det er vanskelig å forutsi omfanget av hvilket inngrep i ytringsfriheten slike filtreringsmetoder faktisk vil innebære. Et krav om filtrering vil videre rette seg mot en mellommann, tilbyderen av internettforbindelsen, og ikke den som faktisk står bak det uønskede innholdet. Etter flertallets oppfatning, bør strafforfølgningen som hovedregel rette seg mot dem som faktisk gjør noe straffbart og ikke mot tjenestetilbyderen som kun tilrettelegger for kommunikasjon. Flertallet er enig med mindretallet i at det bør gjelde tilsvarende regler for ytringer som fremsettes på internett som for ytringer som fremsettes på annen måte. Det store problemet i denne sammenheng er at også lovlig fremsatte ytringer vil bli stoppet i et slikt filter. Flertallet er derfor av den oppfatning at man ved innføring av slik filtrering, i stor grad vil gå på tvers av prinsippene om frihet og åpenhet på internett. Flertallet oppfatter dessuten datakrimkonvensjonen dit hen at målet er ensartet lovgivning hos de ratifiserende stater, med det siktemål at kriminaliteten kan stoppes i opprinnelseslandet. Metoder som filtrering vil på denne bakgrunn heller ikke fremstå som nødvendig.

Etter EMK artikkel 10 andre ledd må et inngrep i ytringsfriheten være i samsvar med lov, ivareta nærmere oppregnede legitime formål og være nødvendig i et demokratisk samfunn. I følge rettspraksis fra den europeiske menneskerettighetsdomstolen, som beskrevet i Erik Møse: «Menneskerettigheter» side 100 er det avgjørende at «staten kan påvise at inngrepet tilsvarer et tvingende samfunnsmessig behov, om det står i forhold til det legitime formål som skal ivaretas, og om de grunner som anføres av de nasjonale myndigheter, er relevante og tilstrekkelige». Flertallet kan ikke se at vilkårene for unntak fra ytringsfrihetene vil være oppfylt all den tid filtrering også medfører store muligheter for at også materiale som ikke er ulovlig faktisk blir stoppet.

Flertallet mener at effekten av en slik ordning vil være begrenset i en slik grad at det i seg selv taler imot ordningen. Det vil være så mange muligheter for å omgå slike filtre at nytteeffekten vil bli sterkt begrenset. Flertallet mener videre at filtreringen i praksis er så unøyaktig at også dette tilsier at man ikke bør gå inn på en slik ordning.

Bruk av filtrering kan for øvrig berøre EØS-avtalen og forbudet mot diskriminering av varer og tjenester innenfor det indre marked, da resultatet kan bli at man, etter en avgjørelse fra domstolen, faktisk sperrer for næringsvirksomhet som er tillatt i andre deler av EØS-området.

Når det gjelder seksualiserte skildringer av barn på internett, er flertallet av den oppfatning at denne type materiale står i en særstilling i forhold til annet uønsket materiale. Det vises i den sammenheng til den frivillige filtreringsordningen for tjenestetilbydere som er beskrevet tidligere. Ordningen innebærer at tilbyderne implementerer et filter som vanskeliggjør tilgang til nettsteder som

inneholder seksualiserte skildringer av barn etter anvisning fra Kripos. Ordningen har således som formål å forhindre tilfeldig tilgang og vanskeliggjøre tilsiktet tilgang til slike seksualiserte skildringer av barn for norske borgere. En forutsetning for at denne ordningen skal fungere, er at det går kort tid fra det avdekkes ulovlig materiale til tilgangen til dette er blokkert. Flertallet er av den oppfatning at tilbyderne vil ønske domstolskontroll ved filtrering dersom det vedtas en lovbestemmelse om dette. På denne måten mener flertallet at en eventuell lovhjemmel faktisk kan svekke en allerede fungerende ordning. Flertallet mener videre at det vil være svært upraktisk og kostnadskrevende om påtalemyndigheten skulle gå via domstolene med begjæring om filtrering for hvert tilfelle som avdekkes av slikt materiale.

Vedtagelse av en lovhjemmel om filtrering vil trolig medføre økte kostnader for både tjenestetilbydere, påtalemyndigheten og domstolene. Alle tjenestetilbydere vil måtte innføre og administrere et teknisk system for å følge opp eventuelle pålegg om filtrering. All den tid filtreringspålegget vil rette seg mot tjenestetilbyderen som en mellommann og ikke gjerningspersonen, fremstår det ikke umiddelbart som naturlig at kostnadene skal dekkes av disse.

### 5.13.4 Medlemmet Willassens særmerknad

*Medlemmet Willassen* mener at mindretallets forslag om filtrering har så vidtrekkende konsekvenser at medlemmet finner grunn til å kommentere det nærmere. Slik dette medlemmet ser mindretallets forslag, innebærer det en sensur av innholdet på internett i statlig regi. Denne sensuren skal gjennomføres ved at påtalemyndigheten fremmer begjæring om filtrering av bestemte internettsteder til domstolene. Domstolene kan så beslutte at filtrering skal finne sted dersom de finner at vilkårene er til stede. Som et alternativt forslag foreslår mindretallet at sensuren skal gjennomføres av et statlig sensurorgan, med mulighet for etterfølgende domstolskontroll. Når det foreligger en beslutning, skal alle norske internettleverandører etter mindretallets forslag pålegges å blokkere de sensurerte internettstedene, slik at norske brukere ikke kan nå dem.

Dette medlem forstår ønsket om å innføre filtrering av internettrafikk for å hindre at straffbart materiale når norske borgere via internett, men mener at problemet er at slik filtrering neppe vil utgjøre noen vesentlig forskjell for de fleste typer straffbart materiale. Det er eksempelvis kjent at utveksling av seksualiserte skildringer av barn (ofte kalt barnepornografi) i stor grad utveksles på internett. Produksjon, besittelse og spredning av slike bilder er straffbart i de fleste land. Utveksling av slike bilder skjer derfor i stor grad i det skjulte. Utfordringen er derfor primært å finne ut hvem som sprer materialet, ikke å hindre at det når norske borgere. I den grad man klarer å avdekke hvor slikt materiale spres fra, er det i de fleste tilfeller uproblematisk å få myndighetene i det aktuelle land til å gripe inn. Det samme vil være tilfelle for andre typer ulovlig innhold, slik som for eksempel opphavsrettslig beskyttet materiale. Siden slikt materiale er ulovlig i de fleste land, foregår spredningen av dette i stor grad i det skjulte. Slik spredning vil det ikke være mulig å filtrere med den foreslåtte fremgangsmåten. Det man da står igjen med som kan filtreres er innholdstyper som er ulovlig i Norge, men lovlig i andre land, slik som for eksempel spilltjenester med pengeinnsats og gevinst.

Etter dette medlemmets syn er det ikke mulig å gjennomføre effektiv filtrering av internett på tilbydernivå. Den filtrering som er praktisk mulig å gjennomføre er blokkering av bestemte IP-adresser i utlandet. Men slik blokkering er ikke vanskelig å omgå. Utenlandske tilbydere av innhold kan omgå filtereringen ved å skifte IP-adresse raskere enn sensurorganet klarer å følge med på. Dette trenger ikke være spesielt raskt, dersom filtrering krever at påtalemyndigheten reiser sak i hvert enkelt tilfelle. Videre kan norske borgere omgå filtreringen ved å benytte utenlandske servere for videresending (såkalte «proxy-servere»). Det kan hevdes at sistnevnte er for vanskelig å gjennomføre for majoriteten av norske brukere, men dette gjelder bare inntil noen (i Norge eller utlandet) tilbyr dette som en kommersiell tjeneste, for eksempel for å skaffe norske brukere lett tilgang til internettsteder for spill. Det står derfor klart for dette medlemmet at selv for innhold som er ulovlig i Norge, men lovlig i andre land, vil filtreringen være lite effektiv. Det er sannsynlig at det vil oppstå et marked for tjenester som omgår filtreringssystemet og at slike tjenester vil bli benyttet av dem som ønsker å få tilgang til internettspill og annet som er filtrert.

Slik dette medlemmet ser det, handler dette i bunn og grunn om hva vi ønsker med internett. Internett fremstår som et unikt verktøy for å fremme samkvem og samhandel mellom nasjonene. Det er i dag en av de fremste mekanismene for å bringe verdens innbyggere tettere sammen og dermed legge grunnlaget for en fredeligere verden. Å innføre statlig sensur og kontroll med hva borgerne i en enkelt stat gjør på internett passer ikke inn i dette mønsteret. Den åpne infrastruktu-

ren som utgjør internett ville bli ødelagt dersom hver enkelt stat skulle innføre sine egne grenseposter i nettet. Dette medlem kan vanskelig se hvorfor Norge som det eneste land i den vestlige verden skulle innføre en slik grensepost. Man vil med en slik grensepost ikke oppnå målet om å hindre at ulovlig materiale tilflyter norske borgere. Det man derimot oppnår er å sende et signal om at Norge ønsker å stå utenfor det åpne informasjonssamfunnet, og ikke ønsker å ta del i internettøkonomien. Et slikt signal tror dette medlemmet neppe Norge ønsker å sende.

### 5.13.5 Mindretallets syn

*Mindretallet, Christensen og Rønning,* mener at en hjemmel for filtrering bør inntas i straffeloven.

Mindretallet viser til Justiskomiteens merknader i Innst. O. nr. 66 (2004-2005), og konstaterer at det i 2007 ikke er alle internettilbydere som deltar i det frivillige filtreringsamarbeidet mot seksualiserte skildringer av barn. For å følge opp Justiskomiteens innstilling bør det derfor foreslås en hjemmel som gir kompetanse til å pålegge resterende internettilbydere å innføre slikt filter.

Foruten seksualiserte skildringer av barn kan det være aktuelt å filtrere andre sider med ulovlig innhold for norske brukere. Mindretallet mener at en hjemmel for filtrering bør utformes generelt, slik at den gir kompetanse til å filtrere annen straffbar virksomhet i tillegg til seksualiserte skildringer av barn. Eksempler på sider med straffbart innhold kan være sider som tilbyr ulovlig pengespill. Mindretallet viser til at flere land planlegger filtrering på dette området. Det kan i enkelte tilfeller også være grunn til å beskytte norske brukere mot nettsteder som forsøker å svindle brukerne, samt mot nettsteder som sprer skadelig programvare. Filtrering kan også tenkes å være et virkemiddel mot nettsider som sprer innhold i strid med rettighetshavers enerett etter åndsverkloven. Dette gjelder både utenlandske nettsteder som selger musikk i strid med de opphavsrettslige regler som gjelder her i landet og i tilfeller hvor musikk kan lastes ned ved hjelp av fildelingsprogrammer.

Mindretallet er enig med flertallet i at et tiltak av denne typen ikke vil gi 100 prosent effekt, pga. tekniske omgåingsmuligheter. Det gjelder imidlertid også alle andre tiltak på datakriminalitetens område. Selv om effekten ikke vil bli 100 prosent ved en filtreringsordning, vil den kunne bli betydelig. Kan man stanse størsteparten av den ulovlige trafikken ved bruk av filter, vil mye være oppnådd.

Når det gjelder nettsider som gir uttrykk for uønskede meninger, vil hensynet til ytringsfriheten begrense hvilke tiltak som kan treffes. Mindretallet er ikke enige med flertallet i at hensynet til ytringsfriheten taler mot å sensurere utenlandske nettsider med straffbart innhold for norske brukere. Mindretallet er også opptatt av at en filtreringsbestemmelse ikke skal sette nye skranker for ytringsfriheten utover ytringsfrihetens eksisterende grenser i Norge. Mindretallet mener imidlertid at det bør gjelde tilsvarende regler for ytringer som fremsettes på internett som for ytringer som fremstilles på annen måte. Mindretallet viser i denne sammenheng til den internasjonale diskusjonen i Internet Governance samarbeidet, der saken også er diskutert. Selv om det fra ulikt hold i Internet Governance samarbeidet har blitt hevdet at filtreringsbestemmelser er problematiske i forhold til ytringsfriheten, er det en nokså samlet oppfatning på myndighetssiden (også fra land vi mener å kunne sammenligne oss med), at det ikke kan være andre regler på internett enn på andre medier. Det må være mulig å forsøke å hindre for eksempel terrorisme, oppfordring til folkehat / rasisme, seksualiserte skildringer av barn og annen ulovlig aktivitet på internett. Mindretallet ser ikke en avgrenset filtreringsbestemmelse som noe vesentlig inngrep i ytringsfriheten, da det utelukkende vil være aktuelt å blokkere innhold som er straffbart etter norsk lov.

Mindretallet ser denne filtreringen som en forlengelse av de hjemler vi har for stengning av innenlandske nettsteder med lovstridig innhold, jf. kapittel 5.12.3. Når det gjelder nettsteder utenfor Norge, vil ikke slike kunne stenges av norske myndigheter på samme måten som nettsteder innenfor rikets grenser. Filtreringshjemmelen vil kunne brukes for å oppnå samme effekt for utenlandske nettsteder. Det er imidlertid viktig at regler om filtrering ikke virker diskriminerende i forhold til utenlandske nettsteder.

Mindretallet tenker seg ikke at en bestemmelse om filtrering skal brukes i stor utstrekning. Etter mindretallets mening skal hjemmelen bare nyttes etter at det er foretatt en proporsjonalitetsvurdering i det enkelte tilfellet mellom det som kan oppnås ved innføring og ulemper (økonomiske og andre kostnader) ved innføring av den konkrete filtreringsordningen. Dette gjelder ikke minst fordi det er fare for at filtreringstiltak kan komme til å ramme mer enn det som er meningen (såkalte falske positive, jf. flertallets merknader).

Mindretallet legger vekt på at reglene om filtrering skal være så lik reglene om inndragning som mulig, og har utformet sitt lovforslag i samsvar med dette, og foreslår bestemmelsen inntatt som § 76 b i ny straffelov.

Bestemmelsen er utformet slik at den ikke bare omfatter websider, men også datamaskiner med fast IP-adresse som tilbyr ulovlig innhold, for eksempel uautorisert deling av musikkfiler, nedlasting av exploits m.v. Ved henvisningen til § 69 tredje ledd, er det gitt anvisning på at det skal foretas en forholdsmessighetsvurdering. Mindretallet mener at den prosessuelle fremgangsmåten må være den samme som ved stengning av nettsteder etter inndragningsbestemmelsene. Det viser til det som er sagt om saksbehandling og partsforhold i kapittel 5.12.3. Særlig vil bestemmelsene i utvalgets forslag til ny § 76a om partsforholdet være av betydning. Før en slik bestemmelse kan tre i kraft, er det kanskje nødvendig med noen mindre justeringer av straffeprosessloven, men mindretallet utformer ikke konkret forslag om dette nå.

Det kan ta noe tid før en slik sak kommer opp for domstolene. I mellomtiden må straffeprosessuelle tvangstiltak kunne brukes på samme måte som ved inndragning. Dette vil etter mindretallets mening sikre at saken om nødvendig kan behandles raskt.

Mindretallet mener at en filtreringsbestemmelse alternativt kan inntas i en eventuell regulering av innhold som sendes over elektronisk kommunikasjonsnett (inkludert kringkasting) og forvaltes av en egnet myndighet, for eksempel Medietilsynet som i dag arbeider med tilgrensende problemstillinger. Siden filtrering berører sentrale verdier som ytringsfrihet, mener mindretallet at slike vedtak, på samme måte som ved inndragning, i siste instans må kunne bringes inn for domstolene. Dersom vedtak om filtrering skal fattes av et tilsyn bør vedtaket derfor kunne være gjenstand for etterfølgende domstolskontroll. Både den som blir pålagt å foreta filtrering og den som eier nettsiden som blir gjenstand for filtrering må ha anledning til å bringe saken inn for domstolene.

Som ny § 76b foreslår mindretallet:

> «Tjenesteyter kan pålegges å blokkere tilgangen til bestemte steder på internett for sine brukere dersom innholdet ville kunne medføre straffansvar utover bøter i Norge. § 69 tredje ledd og § 76a gjelder tilsvarende. De øvrige regler om inndragning gjelder tilsvarende så langt de passer.»

Mindretallet foreslår at bestemmelsen tas inn i inndragningskapittlet, kapittel 13. Dette fordrer at kapitteloverskriften endres til «Inndragning m.v.».

## 5.14 Om straffeloven § 390 a

Straffeloven § 390 a lyder:

> «Den som ved skremmende eller plagsom opptreden eller annen hensynsløs atferd krenker en annens fred eller som medvirker hertil straffes med bøter eller fengsel inntil 2 år.
>
> Offentlig påtale finner bare sted når det begjæres av fornærmede og finnes påkrevet av almene hensyn».

I Delutredning VII er bestemmelsen foreslått videreført i utkastet til § 26-10 Hensynsløs atferd i kapittel 26 om Vern av den personlige frihet og fred, side 339 flg.

Som det er redegjort for i kapittel 3.5.14 og 5.6.7, er straffeloven § 390 a praktisk for å ramme ytringer på internett som krenker en annens fred. Utvalget mener derfor at det er et klart behov for et slikt straffebud og støtter forslaget om å videreføre bestemmelsen. Utvalget antar imidlertid at den nye bestemmelsen bør ha en ordlyd som tydelig tilkjennegir at den kommer til anvendelse også for handlinger som begås ved elektronisk kommunikasjon. I Ot.prp. nr. 18 (2006-2007) Om lov om endringer i straffeloven m.v. (straffebud om å møte et barn med forsett om å begå seksuelt overgrep m.v.) har regjeringen forslått å innta et nytt annet ledd i straffeloven § 201, som gjør det klart at de handlemåter som er beskrevet i nevnte bestemmelse første ledd bokstav a-c, også er straffbar når de begås ved bruk av elektronisk kommunikasjon m.v. Nytt annet ledd i straffeloven § 201 er således foreslått å lyde:

> «Atferd som nevnt i første ledd bokstav b og c anses forøvet overfor noen også når den er forøvet gjennom bruk av telefon, internett eller annen elektronisk kommunikasjon».

Datakrimutvalget antar derfor at det straffebudet i ny straffelov som viderefører straffeloven § 390 a bør inneholde en tilsvarende bestemmelse, og foreslår at følgende setning inntas:

> «Atferd som nevnt i første ledd anses forøvet overfor noen også når den er forøvet gjennom bruk av telefon, internett eller annen elektronisk kommunikasjon».

Dette supplementet kan også inntas i straffeloven § 390 a og lovforslaget utformes i henhold til dette.

# Kapittel 6
# Straffenivå

## 6.1 Strafferammer

I lovutkastet har utvalget valgt strafferammene for de ulike handlingene ut fra en vurdering av handlingenes straffverdighet. Til dels har utvalget tatt utgangspunkt i andre straffebestemmelser i gjeldende straffelov som man anser har tilsvarende straffverdighet. For andre handlinger – som vanskelig kan sammenlignes med bestemmelser i gjeldende straffelov – har utvalget på mer fritt grunnlag gitt et forslag til strafferamme. På tradisjonell måte har utvalget valgt å foreslå relativt vide strafferammer for å fange opp den ulike straffverdighet handlinger som faller innenfor samme straffebestemmelse, kan ha.

Utvalget har sett hen til synspunktene for fastsetting av strafferammer i Ot.prp. nr. 90 (2003-2004) kapittel 11.2 – 11.4. Videre har utvalget tatt hensyn til prosessuell betydning av strafferammene; særlig er det da vilkårene for når ransaking kan skje en har tenkt på, jf. straffeprosessloven § 192, idet ransaking og beslag er meget aktuelt i saker om datakriminalitet. De fleste bestemmelsene i lovutkastet har også strafferammer som er vide nok til å tilfredsstille vilkåret for pågripelse (alle bortsett fra § 2). Utvalget har også sett det slik at de lovbestemmelsene som kan sies å rette seg mot innledende handlinger (§§ 2, 3, 10 og 11) bør ha lavere strafferammer enn bestemmelser som retter seg mot direkte angrep og skadevoldende handlinger.

I lovutkastet er det fire forskjellige strafferammer for «vanlig» overtredelse. Dette er
- bøter eller fengsel inntil 6 måneder (§ 2)
- bøter eller fengsel inntil 1 år (§§ 3, 8, 10, 11, 12 og 14)
- bøter eller fengsel inntil 3 år (§§ 4, 5, 6, 7, 9, 12 (dersom andre skadelige egenskaper), 15 og 16)
- bøter eller fengsel inntil 6 år (§ 13).

Dersom overtredelsen anses som grov (jf. lovutkastet § 18 og nedenfor kapittel 6.2), foreslås det fire ulike strafferammer. Dette er
- bøter eller fengsel inntil 1 år (§ 2)
- bøter eller fengsel inntil 3 år (§§ 3, 8, 10, 11, 14)
- fengsel inntil 6 år (§§ 4, 5, 6, 7, 9, 12, 15 og 16)
- fengsel inntil 10 år (§ 13).

Dersom overtredelsen anses som liten (jf. lovutkastet § 19 og nedenfor i kapittel 6.2), foreslås det to forskjellige strafferammer:
- bøter eller fengsel inntil 6 måneder (§§ 4, 5, 6, 7, 9, 15 og 16)
- bøter eller fengsel inntil 1 år (§ 13).

Den konkrete fastsetting av straff innenfor strafferammene må selvsagt følge alminnelige prinsipper for straffutmåling. Herunder vil de generelle skjerpende og formildende omstendigheter etter straffelovens alminnelige del komme til anvendelse, jf. straffeloven § 60a (organisert kriminalitet), § 61 (gjentakelse) og § 62 (sammenstøt av lovbrudd), og ny straffelov § 79. Videre vil bestemmelser om formildende omstendigheter komme til anvendelse, straffeloven §§ 57, 58 og 59, og ny straffelov § 80. Ut over dette er det i norsk rett ikke gitt generelle bestemmelser om utmåling av fengselsstraff, i motsetning til for utmåling av bøter, jf. straffeloven §§ 27 og 48b og ny straffelov §§ 28 og 53. Gjennom rettspraksis og teori er det imidlertid utpenslet en del momenter som vil ha betydning for straffutmålingen, og slike momenter vil selvsagt gjelde også for disse bestemmelsene etter lovutkastet. Utvalget vil for øvrig bemerke at spørsmålet om det bør innføres generelle regler om hvilke forhold som skal tillegges vekt ved utmåling av straff innenfor de alminnelige strafferammer, har vært utredet. Straffelovkommisjonen konkluderte både i delutredning I, V og VII med at det ikke burde innføres slike regler, men i Ot.prp. nr. 90 (2003-2004) kom Justisdepartementet til at spørsmålet burde undergis ytterligere vurdering (jf. nevnte proposisjon side 154-156). Bakgrunnen var særlig krav fra internasjonale overvåkingsorganer og rettstilstanden i de øvrige nordiske land. Justisdepartementet sendte derfor ut et høringsbrev om dette 31. august 2005, og spørsmålet er så langt utvalget kjenner til, fortsatt til vurdering i departementet.

Uavhengig av om det blir vedtatt generelle bestemmelser om skjerpende og formildende omstendigheter eller ikke, er det visse momenter

som etter rettspraksis vil ha betydning for straffutmålingen. De mest vanlige er langt tidsforløp før rettskraftig dom og ung alder hos gjerningspersonen. Slike omstendigheter vil selvsagt ha betydning for straffutmåling også for datakriminalitet, og må på vanlig måte veies opp mot handlingens alvorlighet, den skaden som er voldt og andre momenter ved handlingen.

Utvalget bemerker også at dersom flere har handlet i samvirke, vil den enkeltes rolle kunne ha betydning for straffutmålingen. Det vises til ny straffelov § 15 som er en generell bestemmelse om medvirkning. På datakrimområdet – på samme måte som for andre lovovertredelser – må medvirkerens handling og rolle vurderes konkret, og det kan meget godt tenkes at den som legger til rette eller psykisk tilskynder en lovovertredelse, kan bedømmes strengere enn den som faktisk foretar selve handlingen («hovedmannen»).

Et annet moment som har betydning for straffutmålingen, er graden av skyld hos gjerningspersonen. Skyldkravet etter datakrimkapitlet er som hovedregel forsett, men etter lovutkastet § 17 er det for noen av bestemmelsene tilstrekkelig at gjerningspersonen opptrådte grovt uaktsomt (§§ 7, 9, 10, 12 annet ledd og 13). For disse overtredelsene vil det ha betydning for straffutmålingen hvilken skyldform som finnes bevist, og videre hvilken grad av skyld man finner bevist innenfor de forskjellige skyldformene. For forsett vil dette være spørsmål om forsettet er grensende ned mot uaktsomhet, om det foreligger «vanlig» forsett eller om det er snakk om skjerpet (kvalifisert) forsett (det vil si hensikt eller overlegg). For grovt uaktsomme overtredelser vil det avhenge av om man finner bevist en uaktsomhet på grensen mot forsett, eller om den grenser nedad mot simpel uaktsomhet.

Som det fremgår av lovutkastet § 17 er det bare for noen av overtredelene utvalget foreslår at skyldkravet settes til grov uaktsomhet. Dette baserer seg på en vurdering av hvilke av overtredelsene det er praktisk å begå ved uaktsomhet sett i forhold til skadepotensialet ved handlingene. For disse overtredelsene tilsier også bevisbyrdereglene at de grovt uaktsomme overtredelsene er straffbare, idet forsett i en del tilfeller er vanskelig å bevise (for å ramme «skjult forsett»).

På den andre siden finner ikke utvalget å ville foreslå at også simpel uaktsomhet skal være straffbar. For det første på grunn av at databruk og tilgang på datatjenester er i en rivende utvikling; til dels forsøker både det offentlige og private tjenesteytere å få brukere over til elektroniske tjenester. Samtidig er det ingen organisert opplæring og en stor del av befolkningen er henvist til selvopplæring. Det bør i en slik situasjon ikke stille svært strenge krav til kyndighet og aktsomhet hos den enkelte. Her vil både kravet til grov uaktsomhet og også kravet til rettsstrid medføre at man ikke kommer i straffansvar for handlinger som man begår på grunn av ukyndighet. For det andre har man i forarbeidene til ny straffelov tatt til orde for at i den grad uaktsomhet er tilstrekkelig for straffansvar, bør det stilles krav om grov uaktsomhet. Det vises til Ot.prp. nr. 90 (2003-2004) side 114-115 med videre henvisninger.

I kravet om grov uaktsomhet ligger at handlingen er svært klanderverdig og at det er grunnlag for sterk bebreidelse, jf. ny straffelov § 23 annet ledd, og Ot.prp. nr. 90 (2003-2004) side 427. Det vises også til Rt. 1970 side 1235 hvor Høyesterett uttalte:

> «For fellelse etter straffelovens § 422, første ledd, kreves grovt uaktsomt forhold. Jeg er enig i herredsrettens forståelse av denne bestemmelse når retten uttaler at det må foreligge en kvalifisert klanderverdig opptreden som foranlediger sterke bebreidelser for mangel på aktsomhet».

Dommen anses som en prinsipiell avgjørelse i forhold til hva som ligger i kravet om grovt uaktsomt forhold.

Utvalget har vurdert om de grovt uaktsomme overtredelsene som gjøres straffbare etter lovutkastet § 17, bør gis en egen strafferamme, som da settes lavere enn strafferammen for de forsettelige forhold etter den aktuelle bestemmelsen. Utvalget er imidlertid kommet til at når straffansvaret knyttes til den grovt uaktsomme handling, i motsetning til simpel uaktsomhet, og strafferammene er såpass vide som i lovutkastet, er det ikke grunn for å fastsette egne strafferammer for uaktsomhetsansvaret. Til sammenligning kan det vises til gjeldende straffelov § 152 b som har samme strafferamme for forsettelige og grovt uaktsomme handlinger, i motsetning til §§ 150, 151, 151 b og 152 som har forskjellige strafferammer for forsettlige og (simpelt) uaktsomme handlinger.

## 6.2 Grovt eller lite datalovbrudd

Utvalget foreslår at det skilles mellom vanlig, liten og grov overtredelse av datakrimkapitlet. Det vises til det som fremgår av Ot.prp. nr. 90 (2003-2004) kapittel 4.1.3 om oppheving av skillet mellom forbrytelser og forseelser og kapittel 4.1.4 om gradering av lovbruddene. Utgangspunktet er «vanlig» overtredelse, men dersom handlingen har visse kjennetegn, jf. lovutkastet § 18 og nedenfor, kan

overtredelsen karakteriseres som «grov». I så fall faller handlingen inn under den skjerpede strafferamme som fremgår av den enkelte bestemmelse.

Ved avgjørelsen av om en handling etter datakrimkapitlet skal anses som grov, skal det etter lovutkastet § 18 særlig legges vekt på den skaden som er voldt eller kunne vært voldt, om lovbruddet er begått ved å bryte en beskyttelse og om gjerningspersonen har hatt eller kunne ha hatt vinning og størrelsen på vinningen. Om hva som nærmere ligger i disse alternativene vises det til merknadene til § 18.

Utvalget er kommet til at samtlige av straffebestemmelsene i lovutkastet bør ha en skjerpet strafferamme for grove overtredelser. Det er store variasjoner i straffverdigheten for handlinger som faller innenfor de forskjellige straffebestemmelsene, og for å kunne ha en realistisk og ikke for høy strafferamme for de «vanlige» overtredelsene, bør man ha en egen ramme for de mest straffverdige handlingene. Dette er også i tråd med blant annet vinningsforbrytelsene i gjeldende straffelov.

Når det gjelder handlinger som anses som lite datalovbrudd, finner imidlertid utvalget ikke grunn for at alle bestemmelsene i lovutkastet har et slikt alternativ. Det vises til at samtlige av bestemmelsene har bøtealternativ i den ordinære strafferamme, som vil være det mest aktuelle for de minst straffverdige overtredelsene. Noen av bestemmelsene har imidlertid en såpass høy øvre strafferamme for de «vanlige» overtredelsene, at utvalget finner det naturlig å ha en egen ramme for de minst alvorlige overtredelsene innenfor bestemmelsene. Det vises til lovutkastet §§ 4, 5, 6, 7, 9, 13, 15 og 16. Som det vil fremgå har utvalget valgt å gi en egen strafferamme for lite datalovbrudd der strafferammen for «vanlig» overtredelse av bestemmelsen er bøter eller fengsel i inntil 3 år eller høyere.

Ved avgjørelsen av om en handling skal anses som lite datalovbrudd, skal det etter lovutkastet § 19 særlig legges vekt på om skadepotensialet er lite og om gjerningspersonen ikke har eller kunne ha hatt vinning. Om hva som nærmere ligger i disse alternativene vises det til merknadene til § 19.

Det bemerkes særskilt at oppregningen av hva som gjør en handling grov eller liten, ikke er uttømmende. Dette fremgår ved uttrykket «legges det *særlig* vekt på». Utvalget vil fremheve at momentene i oppregningen i §§ 18 og 19 verken er nødvendige eller tilstrekkelige for å klassifisere handlingen som grov eller liten, men momentene som er nevnt vil etter utvalgets oppfatning være særlig aktuelle for graderingen. Graderingen beror imidlertid på en helhetsvurdering, og dette innebærer at en handling ikke nødvendigvis graderes opp eller ned selv om et eller flere av momentene som er nevnt forekommer. Om dette vises det også til Ot.prp. nr. 90 (2003-2004) side 58-59.

I motsetning til det som er vanlig etter gjeldende straffelov inneholder ikke lovutkastet § 18 noen henvisning til «andre særdeles skjerpende omstendigheter», jf. for eksempel gjeldende straffelov §§ 232 og 233. I forarbeidene til ny straffelov er en slik lovgivningsteknikk kritisert, bl. a. fordi dette er lite tilfredsstillende fra et informasjonssynspunkt, og i Ot.prp. nr. 90 (2003-2004) side 59 er det uttalt at i bestemmelser om henholdsvis liten og grov overtredelse bør de sentrale momenter for graderingen angis direkte. I tillegg kommer prosessuelle hensyn, ved at det er sikker rett at dersom strafferammen skjerpes ved særdeles skjerpende omstendigheter i sin alminnelighet, innebærer det at det er den skjerpede strafferammen som har betydning for spørsmål av prosessuell karakter. Slike spørsmål er bl. a. foreldelse, henvisningsreglene ved anke (jf. straffeprosessloven § 321) og saksbehandlingen ved anke (bl. a. om lagmannsretten skal settes med lagrette). Det vises til Rt. 1962 side 494.

# Kapittel 7
# Tilleggsprotokollen av 28. januar 2003 (ETS 189)

## 7.1 Innledning

Det internasjonale samfunn har siden vedtakelsen av menneskerettserklæringen i 1948, gjort betydelige fremskritt i bekjempelsen av rasisme, rasediskriminering, fremmedfrykt og relatert intoleranse. En rekke internasjonale menneskerettighetsinstrumenter er vedtatt, herunder FNs rasediskrimineringskonvensjon 1966 og FNs konvensjon om sivile og politiske rettigheter (SP) 1966. Selv om disse konvensjonene trolig har medført vesentlige endringer på området, er likevel den endelige målsetningen om et samfunn fritt for raserelatert intoleranse bare delvis oppnådd.

Tilleggsprotokollen til datakrimkonvensjonen regulerer rasistiske eller fremmedfiendtlige handlinger foretatt ved hjelp av datasystem. Protokollen utvider datakrimkonvensjonens saklige virkeområde slik at konvensjonsbestemmelsene kommer til anvendelse. Årsaken til at datakrimkonvensjonen ikke selv kriminaliserer slike handlinger, er at ytringsfrihetsinnvendinger ble fremsatt av flere delegasjoner under arbeidet med konvensjonen. Innvendingene førte videre til en utrykkelig presisering i protokollens fortale, som fastslår at den ikke er ment å endre nasjonal lovgivning om ytringsfrihet.

Bakgrunnen for særskilt regulering av rasistiske eller fremmedfiendtlige handlinger var en erkjennelse av at revolusjonen innen informasjons- og kommunikasjonsteknologien, særlig internett, har gitt vesentlige muligheter for rask og enkel spredning av krenkende ytringer til et større antall mottakere over et stort geografisk område. Denne effektiviteten i kommunikasjonsmediene kan styrke de skadelige virkningene av handlingen, ved at ytringens gjennomslagskraft øker.

Tilleggsprotokollen er inndelt i fire kapitler; alminnelige bestemmelser (1), tiltak i nasjonal rett (2), forholdet mellom konvensjonen og tilleggsprotokollen (3) og avsluttende bestemmelser (4).

## 7.2 Ytringsfrihetsaspekter

Den grunnlovsvernede ytringsfrihet er i norsk rett nedfelt i Grunnloven § 100, som sist ble endret 2. februar 2006. Ytringsfriheten er også vernet gjennom internasjonale regelverk, herunder Den europeiske menneskerettskonvensjon (EMK) artikkel 10 og FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 19.

Ytringsfriheten skal ivareta samfunnsmessige hensyn og hensyn av betydning for enkeltmenneskets utfoldelse (demokratihensyn, sannhetshensyn og autonomihensyn). Retten til ytringsfrihet omfatter meddelelsesfrihet (den klassiske frihet til å fremsette ytringer av ethvert innhold), retten til å forholde seg taus, informasjonsfrihet (frihet til å gjøre seg kjent med opplysninger, ideer og budskap som andre frivillig avgir), informasjonskrav (frihet til å motta informasjon) og infrastrukturkrav (statens forpliktelser til aktivt å medvirke til at individene har faktisk ytringsfrihet).

Grunnloven § 100 gir vern mot inngrep i ytringsfriheten fra staten, andre offentlige myndigheter og private rettssubjekt, men rekkevidden av vernet må avveies mot andre vernede interesser. Det er herunder på det rene at lovgivning som for eksempel verner mot blasfemiske, rasistiske og hatefulle ytringer kan tale for en innskrenking av ytringsfriheten etter en konkret vurdering. Det følger imidlertid av grunnlovsbestemmelsen at ansvaret i så fall må være hjemlet i lov, men kravet må etter høyesterettspraksis nyanseres ut ifra hvor omfattende inngrep i ytringsfriheten det er tale om. Det følger også av § 100 at begrensninger i ytringsfriheten må rettferdiggjøres og herunder baseres i klart definerte og forankrede hensyn av tungtveiende art.

Det er på det rene at ytringer av den art som reguleres i tilleggsprotokollen reiser vanskelige og prinsipielle spørsmål i forhold til ytringsfrihetens grenser. Denne problemstillingen ble identifisert av Ytringsfrihetskommisjonen i NOU 1999: 27, der utvalget fremhevet:

> «Hatefulle ytringer representerer et av de vanskeligste og mest kontroversielle områder i forbindelse med ytringsfrihetens grenser, og spørsmålet har vært underkastet gjentatte og lange debatter i kommisjonen. Det er i denne sammenheng nødvendig først å minne om den egentlige begrunnelse for ytringsfrihet i vårt

samfunn. Ytringsfriheten er knyttet til eksistensen av et offentlig rom. Det forutsettes at friheten til å ytre seg i dette rom fører til utluftning, renselse og anstendiggjøring av standpunkter gjennom samtale og kritikk. For at offentligheten skal fungere på denne måten, må de diskriminerende holdninger komme til uttrykk, for det er først når de er uttrykt, at de kan bekjempes gjennom offentlig kritikk. I prinsippet er altså ytringsfrihet tenkt som et vern mot slike fenomener som diskriminering. I det større historiske perspektiv er det heller ikke tvilsomt at det i de åpne samfunn med høy grad av ytringsfrihet har vært mindre grad av diskriminering enn i de lukkede samfunn. Ytringsfrihet har i de fleste tilfeller fungert som et vern mot diskriminering, om enn ikke i alle tilfeller.» (NOU 1999: 27, kapittel 6.3.3.4)

Det er etter utvalgets syn ikke tvilsomt at de forslag til endringer i nasjonal rett som Ytringsfrihetskommisjonen fremmet i NOU 1999: 27, har ført til en betydelig styrking av ytringsfriheten i Norge.

## 7.3 Alminnelige bestemmelser – kapittel I

### 7.3.1 Formål – artikkel 1

Tilleggsprotokollen artikkel 1 avgrenser protokollens formål og lyder:

> «The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as «the Convention»), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.»

Hovedformålet med tilleggsprotokollen er etter ordlyden å harmonisere medlemslandenes materielle straffebestemmelser på dette området, i tillegg til å gi datakrimkonvensjonens prosessuelle og internasjonale samarbeidsbestemmelser anvendelse. Det siste hensynet er trolig det mest sentrale, all den tid et vesentlig antall medlemsland allerede har kriminalisert fremsettelse av rasistiske og fremmedfiendtlige ytringer i nasjonal rett, mens det på den annen side ikke finnes effektive internasjonale samarbeidsmekanismer som kan sikre effektiv etterforskning og påtale.

Forpliktelsene nedfelt i tilleggsprotokollen omfatter både plikt til å innføre tilstrekkelig minimumsvern og plikt til å sikre at lovgivningen blir tilstrekkelig håndhevet.

Protokollens artikkel 3-5 kriminaliserer nærmere bestemt fremsettelse av «rasistisk eller fremmedfiendtlig» materiale ved hjelp av datasystem. Disse bestemmelsene er plassert i protokollens kapittel om tiltak som må gjennomføres i nasjonal rett, og det er derfor av betydning å se nærmere på hva som ligger i dette begrepet. Det er imidlertid verdt å fremheve at medlemslandene ikke plikter å innføre definisjonen som fremgår av artikkel 2 (1) i nasjonal rett. Dette følger av artikkelens plassering i protokollens kapittel 1.

### 7.3.2 Definisjon – artikkel 2

Tilleggsprotokollen artikkel 2 (1) gir følgende definisjon av hvilke typer ytringer som anses «rasistisk og fremmedfiendtlig»:

> ««racist and xenophobic material» means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.»

Artikkel 2 (1) gir etter ordlyden en vid definisjon av hvilket materiale som anses «rasistisk eller fremmedfiendtlig». Både skriftlig materiale, bilder og enhver representasjon av ideer eller teorier omfattes, såfremt dette fremmer eller oppfordrer til hat, diskriminering eller vold mot individer eller grupper av individer, på bakgrunn av rase, hudfarge, nedstamning og/eller nasjonal/etnisk opprinnelse. På samme måte kan ytringer om noens religion omfattes, forutsatt at ytringen brukes som et påskudd i denne kontekst.

Definisjonen i artikkel 2 viser til de mulige *konsekvenser* av fremsettelsen, og det avgjørende etter definisjonen er, ifølge Europarådets forklarende rapport til protokollen (side 3), at materialet *kan* gi den nærmere bestemte effekt. Det kreves etter dette ingen påviselige skadevirkninger etter bestemmelsen, selv om ordlyden isolert sett kan tolkes i denne retning.

Begrepet «vold» omfatter uberettiget bruk av makt, mens begrepet «hat» omfatter intens misbilligelse. Ordet «diskriminering» skal etter den forklarende rapporten (side 3) fortolkes i samsvar med Den europeiske menneskerettskonvensjon (EMK) artikkel 14 og protokoll 12, Menneskerettsdomstolens (EMDs) praksis på området og FNs rasediskrimineringskonvensjon artikkel 1. I denne kontekst omfatter begrepet enhver uberettiget forskjellsbehandling av personer eller gruppe av per-

soner på grunnlag av visse karakteristika. EMD har gjennom rettspraksis uttalt at en forskjellsbehandling er diskriminerende, når den ikke har noen nøytral og rimelig berettigelse, det vil si at den ikke forfølger et legitimt formål eller ikke er proporsjonal, sett i forhold til de anvendte virkemidler og målet som søkes oppnådd.

Et ytterligere vilkår i artikkel 2 er at de negative følgene «hat», «diskriminering» eller «vold» må knyttes til et individ eller gruppe av individer, på grunnlag av rase, hudfarge, nedstamning, religion eller nasjonalt eller etnisk opphav. Det fremgår av tilleggsprotokollens forklarende rapport (side 4) at disse grunnlagene må fortolkes med utgangspunkt i både nasjonal og internasjonal rett, men begrepene krever likevel en viss presisering i tilknytning til tilleggsprotokollen.

Begrepet «nedstamning» refererer i hovedsak til personer eller gruppe av personer som nedstammer fra personer som kan identifiseres ved nærmere bestemte karakteristikker, så som rase eller hudfarge, selv om disse karakteristikkene ikke nødvendigvis eksisterer eller gjør seg gjeldende i dag. Det avgjørende er følgelig om de fremsatte karakteristikkene utsetter de aktuelle personene for hat, diskriminering eller vold, som følge av tilknytningen. Sosial tilhørighet omfattes imidlertid ikke av begrepet.

Begrepet «nasjonalt opphav» skal ifølge den forklarende rapporten (side 4) fortolkes utvidende, og omfatter ytringer om den nasjonale tilhørighet eller opphavet til individet selv eller individets forfedre. Vilkåret kan være oppfylt selv om den som utsettes for krenkelsen rettslig sett ikke lenger har den nasjonale tilhørighet, så som statsløse personer og personer med dobbelt statsborgerskap. Begrepet omfatter på samme måte ytringer om minoriteter eller annen gruppe av personer uten tilknytning til internasjonalt anerkjent nasjon.

Artikkel 2 fastsetter avslutningsvis at ytringer om noens «religion» kan omfattes av definisjonen. Begrepet referer til religiøs overbevisning eller tro, men skal ifølge den forklarende rapporten (side 4) ikke tolkes utvidende. Det avgjørende etter bestemmelsen er hvorvidt ytringer om noens religion brukes som en forutsetning – eller påskudd for ytringer om noen av de øvrige grunnlagene i artikkel 2, for eksempel rase eller hudfarge.

## 7.4 Tiltak i nasjonal rett – kapittel II

### 7.4.1 Tilleggsprotokollens overensstemmelse med norsk rett

Tilleggsprotokollens kapittel 2 pålegger medlemslandene å kriminalisere nærmere bestemte ytringer. Det er verdt å bemerke at samtlige bestemmelser krever at handlingene har blitt foretatt «intentionally and without right». Det fremgår av den forklarende rapporten (side 5) at det overlates til de enkelte medlemslandene å fastsette det nærmere innholdet i disse vilkårene, som refererer seg til det alminnelige forsettskravet og rettstridsreservasjonen i strafferetten.

Tilleggsprotokollen regulerer kun handlinger foretatt ved hjelp av «datasystem». Dette begrepet skal tolkes på samme måte som etter datakrimkonvensjonen. Begrepet er belyst i kapittel 5.2 og 9.1.

### 7.4.2 Spredning av rasistisk eller fremmedfiendtlig materiale- artikkel 3

*Innledning*

Artikkel 3 rammer spredning av krenkende materiale og fastsetter følgende:

«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.
3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.»

Artikkelen pålegger statene å kriminalisere distribusjon eller annen tilgjengeliggjøring av rasistisk eller fremmedfiendtlig materiale til allmennheten («to the public»). Spredning til allmennheten anses ikke skjedd der ytringene fremsettes i privat korrespondanse, for eksempel fra en sender til en

mottaker via elektronisk post. Publisering av ytringene på allment tilgjengelige nettsteder, diskusjonsfora og nyhetsgrupper vil derimot omfattes av begrepet.

Spredning av ytringer på tjenester som krever autorisering (for eksempel passordbelagte nettsider), vil også rammes av artikkel 3, all den tid materialet gjøres tilgjengelig for enhver. Forutsetningen er imidlertid at autorisering gis til alle som fyller visse kriterier, typisk ved at brukeren registrerer seg med et brukernavn, en oppgitt alder og/eller en elektronisk postadresse.

Den forklarende rapporten (side 6) fastsetter at det avgjørende vurderingstema ved klassifiseringen av spredningshandlingen er hvorvidt avsenderen hadde til hensikt å spre materialet til allmennheten. Hvis avsenderen sendte materialet til en enkelt privat e-postmottaker, vil vilkåret eksempelvis ikke være oppfylt selv om materialet senere publiseres på en allment tilgjengelig tjeneste av andre enn avsenderen. Den subjektive vurdering må her som ellers imidlertid skje på bakgrunn av de ytre omstendigheter. Objektivt konstaterbare forhold som ytringens innhold, hvilken teknologi eller programvare som er brukt for å fremsette ytringen, om sikkerhetstiltak er benyttet for å skjerme innholdet (kryptering etc.), og konteksten ytringen ble fremsatt i, er sentrale momenter i denne vurderingen. På samme måte vil antallet mottakere av ytringen og hvilken forbindelse disse har til avsenderen være relevant å få avklart når avsenderens subjektive forhold skal vurderes.

Den aktuelle spredningshandlingen (distribusjon eller annen tilgjengeliggjøring) omfatter etter den forklarende rapporten (side 5) enhver aktiv direktespredning av materialet, for eksempel publisering av ytringene i allment tilgjengelige chatterom, nyhetsgrupper eller andre diskusjonsfora. Også indirekte spredning av materialet gjennom hyperlenking (snarveier) til materialet er ment å omfattes av artikkelen, forutsatt at de subjektive vilkår er oppfylt. Det er i denne sammenheng verdt å fremheve at forsettskravet etter bestemmelsen må dekke både spredningshandlingen og materialets rasistiske eller rasediskriminerende innhold.

Artikkel 3 (3) gir medlemslandene begrenset rett til ikke å straffbelegge spredningen når ytringene ikke fremmer hat eller vold og landet tilbyr andre rettsmidler, for eksempel sivilrettslige eller administrative midler. Medlemslandene kan videre velge å benytte reservasjonsretten av hensyn til etablerte ytringsfrihetsprinsipper. Reservasjonen kan imidlertid innskrenkes ved at det fastsettes i nasjonal rett at de ytringer som rammes for eksempel fornærmer, nedverdiger eller truer en gruppe personer.

*Straffeloven § 135 a*

Straffeloven § 135 a straffbelegger offentlig fremsettelse av diskriminerende eller hatefulle ytringer og lyder:

> «Den som forsettlig eller grovt uaktsomt offentlig setter frem en diskriminerende eller hatefull ytring, straffes med bøter eller fengsel inntil 3 år. Likt med en offentlig fremsatt ytring, regnes en ytring når den er satt frem slik at den er egnet til å nå et større antall personer, jf. straffeloven § 7 nr. 2. Som ytring regnes også bruk av symboler. Medvirkning straffes på samme måte.
>
> Med diskriminerende eller hatefull ytring menes det å true eller forhåne noen, eller fremme hat, forfølgelse eller ringeakt overfor noen på grunn av deres
> a) hudfarge eller nasjonale eller etniske opprinnelse,
> b) religion eller livssyn, eller
> c) homofil legning, leveform eller orientering.»

Bestemmelsen fikk sitt nåværende innhold ved lov av 3. juni 2005 nr. 33 og trådte i kraft 1. januar 2006. Straffbare ytringer ble på dette området tidligere regulert i loven § 135, annet ledd, men Norges tiltredelse av FN-konvensjonen om avskaffelse av alle former for rasediskriminering av 21. desember 1965 førte til at denne bestemmelsen ble opphevet. Den gjeldende § 135 a utvider bestemmelsens rekkevidde og har som hovedformål å gi visse utsatte grupper vern mot krenkende ytringer, herunder hindre spredning og utbredelse av rasistiske ytringer.

I rettspraksis er straffeloven § 135 a tolket innskrenkende av hensyn til Grunnloven § 100 og EMK artikkel 10, senest i Rt. 1997 side 1821 («Kjuus») og Rt. 2002 side 1618 («Sjølie»). I avgjørelsen fra 2002 presiserer Høyesterett forholdet mellom Grunnloven § 100 og § 135 a slik:

«§135 a [...] må uten videre anvendes med de begrensninger som følger av Grunnloven § 100. [...] § 135 a [...] rammer ytringer av kvalifisert krenkende karakter. Utsagn som oppfordrer eller gir tilslutning til integritetskrenkelser, vil kunne være av en slik karakter. Et annet moment vil være om utsagnene innebærer en grov nedvurdering av en gruppes menneskeverd. Negative utsagn og meningsytringer av typen «Norge for nordmenn» vil på den annen side være vernet av ytringsfriheten. Det er ikke noe krav om at utsagnene skal ha utsatt noen for skade.»

Etter lovteksten i § 135 a rammes ytring som er «diskriminerende eller hatefull». Både muntlige og skriftlige ytringer omfattes av ordlyden så vel som realakter. Det følger også av bestemmelsen at bruk av symboler kan rammes. De konkrete ytringer som omfattes er nærmere opplistet i andre ledd. Lovtekstens ordlyd rammer ikke utrykkelig ytringer knyttet til «rase», men det følger av Ot.prp nr. 33 (2004-2005), side 215, at slike ytringer er ment å omfattes av § 135 a annet ledd bokstav a. Utvalget antar videre at ytringer om noens «nedstamning», kan innfortolkes i dette alternativet, jf. tilleggsprotokollens artikkel 2 og kommentarene til denne i kapittel 7.3.2.

Det følger av rettspraksis at § 135 a ikke stiller vilkår om skadevirkning for at ytringen skal kunne rammes. Det avgjørende etter praksis er hvorvidt ytringen kan anses «kvalifisert krenkende» etter en konkret vurdering. Utvalget har tidligere påpekt at heller ikke artikkel 3 i tilleggsprotokollen stiller krav om skadevirkning. Det avgjørende etter artikkel 3 er hvorvidt ytringene *kan* gi en nærmere bestemte effekt, ikke om de faktisk gjør det.

Ytringene må imidlertid etter § 135 a annet ledd true eller forhåne noen, eller fremme hat, forfølgelse eller ringeakt overfor noen for å anses diskriminerende eller hatefullt. Det følger av rettspraksis at hat, forfølgelse eller ringeakt er sterke karakteristikker og at det derfor kun er de grove forhold som rammes, jf. Rt. 1997 side 1821 («Kjuus»). Utvalget antar likevel at ordlyden dekker tilleggsprotokollens vilkår «hat, diskriminering eller vold», jf. artikkel 2.

Ytringen må for å kunne rammes av § 135 a, ha vært offentlig fremsatt eller satt frem slik at den er egnet til å nå et større antall personer. I siste tilfelle regnes ytringen som offentlig fremsatt. Straffeloven § 7 nr. 2 angir når handlingen kan sies å være forøvet offentlig og vil derfor være relevant. Utvalget viser i denne sammenheng også til den nye straffeloven § 10. Det kreves etter ordlyden i § 135 a imidlertid ikke at ytringen rent faktisk ble offentlig fremsatt, hvis ytringen kunne ha blitt sett eller hørt av et tilstrekkelig antall personer. Det vil i denne sammenheng være av betydning hvor, når og på hvilken måte ytringen ble fremsatt. Ytringer som ved bruk av et datasystem, er publisert på en nyhetstjeneste eller nettside på internett vil eksempelvis kunne rammes selv om ingen faktisk har sett eller hørt ytringen. Endringen av § 135 a til også å omfatte andre ytringer enn de som rent faktisk er offentlig fremsatt, bygger på forslaget til definisjon av offentlig handling i § 10 i den nye straffeloven, jf. Ot.prp. nr. 90 (2003-2004) side 408-409. Utvalget antar at bestemmelsens vilkår dekker vilkåret om spredning til allmennheten («to the public») etter tilleggsprotokollens artikkel 3.

Skyldkravet etter straffeloven § 135 a er forsett eller grov uaktsomhet, og er følgelig mer vidtfavnende enn skyldkravet etter tilleggsprotokollens artikkel 3.

### *Behovet for endringer i nasjonal rett*

Den europeiske kommisjonen mot rasisme og intoleranse (ECRI) er et uavhengig organ opprettet av Europarådet. ECRI skal overvåke menneskerettigheter og består av uavhengige medlemmer med ekspertkunnskap om rasisme, fremmedfiendtlighet, antisemittisme og intoleranse. ECRIs arbeid fokuseres på de enkelte medlemslandene i Europarådet og en sentral oppgave er å rapportere om situasjonen i de enkelte land og herunder gi forslag til hvordan eventuelle påviste nasjonale problemer kan håndteres.

ECRI vedtok den 27. juni 2003 sin 3. rapport om Norge og identifiserte der problemer med gjennomføringen av straffeloven § 135 a. Det ble fremhevet at rettssystemets sterke vektlegging av ytringsfriheten hadde gått på bekostning av andre rettigheter. Dette hadde ifølge ECRI ført til at enkeltpersoner ikke ble gitt tilstrekkelig vern mot rasistiske ytringer. Kommisjonen viste i denne sammenheng til plenumsavgjørelsen i Rt. 2002 side 1618 («Sjølie»). FNs rasediskrimineringskomité har også tidligere kritisert denne avgjørelsen fra Høyesterett og ga utrykk for at domstolens rettsforståelse er i strid med FNs rasediskrimineringskonvensjon artikkel 4.

Straffeloven § 135 a har blitt endret siden publiseringen av ECRIs rapport og kritikken fra FNs rasediskrimineringskomité. Den vesentligste endringen er at bestemmelsens rekkevidde er utvidet. Hovedformålet var å gi utsatte grupper et mer effektivt vern mot krenkende ytringer. Skyldkravet ble videre endret, slik at grov uaktsomhet er tilstrekkelig for overtredelse. Vurderingen vil etter endringen i større grad derfor kunne knyttes til selve handlingen uavhengig av siktedes tankeprosess.

Utvalget er av den oppfatning at straffeloven § 135 a i nåværende utforming dekker forpliktelsene etter tilleggsprotokollens artikkel 3. Den nærmere grensedragning mellom ytringsfriheten og vernet mot krenkende ytringer må som tidligere trekkes opp gjennom rettspraksis.

### 7.4.3 Rasistiske eller fremmedfiendtlige trusler – artikkel 4

*Innledning*

Artikkel 4 regulerer rasistisk eller fremmedfiendtlig motivert trussel og fastsetter følgende:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
>
> threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.»

Artikkelen pålegger statene å straffbelegge rasemotivert eller fremmedfiendtlig trussel som fremsettes ved hjelp av datasystem. Det erkjennes imidlertid i Europarådets forklarende rapport (side 6) at de fleste av Europarådets medlemsland allerede har lovgivning som gir generelt vern mot trusler, men at artikkel 4 skal sikre at det ikke foreligger tvil om at intern rett faktisk omfatter rasistisk eller fremmedfiendtlige trusler.

Den forklarende rapporten presiserer at begrepet «trussel» omfatter ytringer som skaper frykt for å bli utsatt for alvorlige straffbare handlinger hos trusselens adressat(er) eller adressatens familie («relatives»). Det overlates herunder til medlemslandenes nasjonale lovgivning å definere hva som skal regnes som «alvorlig straffbar handling» («serious criminal offence»), men rapporten fastsetter at krenkelser av den personlige sikkerhet, integritet eller private eiendom, vil ligge i artikkelens kjerneområde.

Det fremheves videre i rapporten at trusselen ikke trenger å være fremsatt offentlig for å rammes. Trusler gjennom privat kommunikasjon vil følgelig kunne rammes av artikkel 4.

*Straffeloven § 227*

Straffeloven § 227 fastsetter følgende:

> «Med Bøder eller med Fængsel indtil 3 Aar straffes den, som i Ord eller Handling truer med et strafbart Foretagende, der kan medføre høiere Straf end 1 Aars Hefte eller 6 Maaneders Fængsel, under saadanne Omstændigheder, at Truselen er skikket til at fremkalde alvorlig Frygt, eller som medvirker til saadan Trusel.
>
> Under særdeles skjerpende omstendigheter, jf. § 232 tredje punktum, kan fengsel inntil 6 år idømmes.»

Som det fremgår av bestemmelsen, rammer ikke straffeloven § 227 enhver trussel. Bestemmelsen krever at det trues med en straffbar handling («strafbart Foretakende») av en viss alvorlighet (handlinger som kan "medføre høiere Straf end [...] 6 Maaneders Fængsel"). Man må dermed se på hva det trues med; om dette er straffbart, og i så fall hvilken strafferamme forholdet har etter loven (straffeloven eller særlovgivningen). Trusler om vold vil falle inn under § 227 dersom det trues med legemsbeskadigelse (straffeloven § 229) eller alvorligere voldshandlinger, men ikke legemsfornærmelse (straffeloven § 228 første ledd, som har en strafferamme på bøter eller 6 måneders fengsel). Trusler om tvang (§ 222), kidnapping (§ 223) eller skadeverk (§ 291) er også eksempler som er straffbare etter § 227. Det fremgår av rettspraksis at det ikke stilles krav om at trusselen må være fremsatt direkte overfor den som trusselen skal gå ut over, jf. for eksempel Rt. 1984 side 1197.

Det fremgår videre av § 227 at trusselen må være «skikket til at fremkalde alvorlig Frygt». Vilkåret henspeiler til en objektiv vurdering av hvorvidt trusselen er egnet til å fremkalle alvorlig frykt, basert på trusselens innhold og de omstendigheter den er fremsatt under. Det vises i denne sammenheng til Innst. O. VI (1889) side 23. Det kreves motsetningsvis ikke at fornærmede faktisk har følt seg truet, jf. blant annet Rt. 1981 side 970.

Dersom en trussel som faller inn under straffeloven § 227 er rasistisk motivert (eller det foreligger andre særdeles skjerpende omstendigheter, jf. straffeloven § 232 tredje punktum), innebærer dette at den strengere strafferammen i § 227 annet straffalternativ kommer til anvendelse. Alternativet «rasistisk motivert» omfatter nedlatende eller fiendtlige holdninger overfor enkeltpersoner eller grupper personer på grunnlag av deres rase, hudfarge eller nasjonale eller etniske opphav.

*Behovet for endringer i nasjonal rett*

Straffeloven § 227 gir en vid hjemmel for å straffe trusler i norsk rett. Av rettspraksis fremgår det at det skjerpede strafferammen benyttes når en trussel bedømmes som rasistisk eller fremmedfiendtlig, jf. for eksempel Rt. 1994 side 1604 og Rt. 1994 side 974. Begrensningen i § 227, ved at den kun straffbelegger trusler om straffbare handlinger med strafferamme over 6 måneder, antas ikke å innebære at bestemmelsen er snevrere enn det

som kreves etter tilleggsprotokollen artikkel 4. Det vises til at tilleggsprotokollens forklarende rapport presiserer at begrepet "trussel" i artikkel 4 omfatter ytringer som skaper frykt for å bli utsatt for alvorlige straffbare handlinger.

Utvalget er etter dette av den oppfatning at oppfyllelse av forpliktelsene etter artikkel 4 ikke nødvendiggjør endringer i straffeloven. Utvalget antar videre at rasistiske trusler som fremsettes offentlig også kan rammes av straffeloven § 135 a.

### 7.4.4 Rasistisk eller fremmedfiendtlig fornærmelse – artikkel 5

*Innledning*

Tileggsprotokollen artikkel 5 regulerer fremsettelse av rasistisk eller fremmedfiendtlig fornærmelse, og fastsetter følgende:

«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2. A Party may either:
   a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or
   b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.»

Artikkelen regulerer offentlig fremsatt fornærmelse av personer eller gruppe av personer fordi disse tilhører, eller er antatt å tilhøre en gruppe kjennetegnet ved visse karakteristikker (rase, hudfarge, nedstamming, etnisk eller nasjonalt opphav, eller religion hvis dette brukes som et påskudd til å fremme ytringer om noen av de øvrige faktorene).

Begrepet «fornærmelse» («insult») refererer ifølge Europarådets forklarende rapport (side 6), til enhver anstøtelig, foraktelig eller hånlig ytring som kan krenke adressatens æresfølelse eller verdighet. Det fastsettes herunder at fornærmelsen må være direkte knyttet til adressatens tilhørighet til den aktuelle gruppen.

Artikkelen rammer i motsetning til trusler etter artikkel 4, kun fornærmelser som er offentlig («publicly») fremsatt. Fornærmelser gjennom privat kommunikasjon, for eksempel i en e-post til adressaten, faller følgelig utenfor artikkel 5.

Artikkel 5 nr. 2 bokstav a gir medlemslandene mulighet til å fastsette vilkår om at handlingen faktisk (ikke bare potensielt) utsetter adressaten(e) for hat, ringeakt eller hån. Reservasjonsretten i artikkel 5 nr. 2 bokstav b kan videre alternativt benyttes så vidt at medlemslandet reserverer seg helt eller delvis i forhold til artikkel 5 nr. 1.

*Straffelovens bestemmelser*

Straffeloven har ingen klare paralleller til tilleggsprotokollen artikkel 5, men utvalget antar at § 135 a kan ramme offentlig fremsettelse av fornærmelser når denne har diskriminerende eller hatefullt innhold av kvalifiserende art. Straffeloven § 390 a kan også dekke noe av artikkel 5s virkeområde, da den rammer «skremmende eller plagsom oppførsel eller annen hensynsløs atferd krenker en annens fred». Siden artikkel 5 hovedsaklig verner adressatens æresfølelse, antar utvalget videre at straffeloven §§ 246 flg. kan ramme slike ytringer.

*Behovet for endringer i nasjonal rett*

Utvalget antar at straffeloven § 135 a, § 390 a og bestemmelsene om ærekrenkelser i §§ 246 flg. dekker forpliktelsene etter tilleggsprotokollens artikkel 5. Det foreligger etter utvalgets oppfatning følgelig ikke behov for å endre straffeloven eller benytte reservasjonsretten.

### 7.4.5 Fornektelse, vesentlig minimalisering, aksept eller forsvar av folkemord eller forbrytelser mot menneskeheten – artikkel 6

*Innledning*

Flere europeiske domstoler har i løpet av de senere år behandlet saker der personer har blitt strafforfulgt for å ha fornektet, minimalisert eller utrykt seg positivt om krigsforbrytelser eller andre forbrytelser mot menneskeheten. Den kjente britiske forfatteren David Irving ble for eksempel domfelt og fengslet i 2006 av en domstol i Østerrike for å ha fornektet at Holocaust fant sted under den 2. verdenskrig. David Irving hadde i 1989 fremsatt ytringene i to foredrag han holdt på østerriksk statsterritorium.

De ytringer som i praksis har vært fremmet i denne kontekst, er ofte presentert som resultater

av seriøs vitenskapelig forskning og brukes i stor grad av høyreekstreme grupperinger av forskjellig art for å underbygge rasistiske og fremmedfiendtlige budskap. Slike grupperinger benytter i vesentlig omfang internett som kommunikasjonsmedium.

Tilleggsprotokollens artikkel 6 ble nedfelt for å verne personer eller minnet om personer som har blitt utsatt for den aktuelle begivenhet, og således beskytte den menneskelige verdighet. Artikkel 6 fastsetter følgende:

«1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:
distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.
2. A Party may either
a) require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.»

Artikkel 6 regulerer ytringer om folkemord eller andre forbrytelser mot menneskeheten. Det fremgår av bestemmelsen at internasjonal rett og rettspraksis fra anerkjente krigstribunal og straffedomstoler har betydning for klassifiseringen av hva som omfattes av disse begrepene. Artikkel 6 ble primært gitt med sikte på klart etablerte historiske begivenheter som fant sted under den 2. verdenskrig, men det er på det rene at ytringer om begivenheter fra den senere tid også vil kunne rammes.

Artikkel 6 nr. 2 fastsetter at medlemslandene kan fastsette vilkår om at handlingen etter første punkt kun gjøres straffbar når ytreren hadde til hensikt å skape hat, diskriminering eller vold mot individer eller gruppe av individer, basert på rase, hudfarge, nedstamming, nasjonalt eller etnisk opphav, eller religion hvis dette brukes som påskudd i denne kontekst. Bestemmelsen gir i artikkel 6 nr. 2 bokstav b medlemslandene rett til å reservere seg helt eller delvis.

### *Internasjonalt*

En rekke europeiske land har allerede etablert nasjonal lovgivning som regulerer ytringer om klart etablerte historiske begivenheter knyttet til folkemord eller forbrytelser mot menneskeheten.

Den franske Loi Gayssot-loven fra 1990 forbyr rasistiske, antisemittiske eller fremmedfiendtlige ytringer. Belgia har liknende lovgivning som forbyr såkalt hatefull omtale. Andre europeiske land som har lovregulert Holocaust-fornektelse omfatter Sveits, Tyskland, Østerrike, Romania, Slovakia, Den Tsjekkiske Republikk, Litauen og Polen.

Det svenske lovutvalget som vurderte om Sverige skal tiltre tilleggsprotokollen har av hensyn til ytringsfriheten imidlertid gått inn for å benytte reservasjonsadgangen etter artikkel 6 nr. 2 bokstav b. Det vises i denne sammenheng til det svenske lovutvalgets utredning «Brott og brottsutredning i IT- miljø: Europarådets konvention om IT-relaterad brottslighet med tilleggsprotokoll», av 23. februar 2005. Danmark har også reservert seg etter tilleggsprotokollens artikkel 6 nr. 2 bokstav b ved ratifisering av protokollen.

### *Norsk rett*

Straffeloven gir ingen utrykkelige bestemmelser om fornektelse, vesentlig minimalisering, aksept eller forsvar av folkemord eller forbrytelser mot menneskeheten, men utvalget antar at slike ytringer kan rammes av straffeloven § 135 a dersom ytreren i denne sammenheng forsettlig eller grovt uaktsomt offentlig fremsetter en diskriminerende eller hatefull ytring. Utvalget er herunder av den oppfatning at ytringer som fornekter, vesentlig minimaliserer, aksepterer eller forsvarer folkemord eller forbrytelser mot menneskeheten etter en konkret vurdering, nok kan rammes av gjerningsbeskrivelsen i § 135 a, forutsatt at de er kvalifisert krenkende. Utvalget har imidlertid kommet til at § 135 a ikke oppfyller forpliktelsene i tilleggsprotokollens artikkel 6 nr. 1. Straffeloven § 135 a rammer ytringer som truer, forhåner, fremmer hat, forfølgelse eller ringeakt overfor noen, og artikkel 6 nr. 1 stiller ikke opp tilsvarende vilkår. § 135 a skal etter endringen som trådte i kraft 1. januar 2006, riktignok gi et bedre vern mot grove rasis-

tiske og andre krenkende ytringer, men den vil etter omstendighetene fortsatt måtte tolkes innskrenkende av hensyn til ytringsfriheten. Det er også på det rene at tidligere rettspraksis knyttet til § 135 a fortsatt vil ha relevans, og terskelen for inngrep er etter denne praksis høy. Det fremgår herunder at det bare er ytringer med sterke karakteristikker av grov karakter som rammes, jf. Rt. 1997 side 1821, og det skal vektlegges om man befinner seg på et område hvor hensynet til ytringsfriheten har mindre vekt enn normalt, jf. Rt. 1994 side 768. Utvalget er av den oppfatning at ytringer om historiske begivenheter normalt ikke faller i en kategori hvor ytringsfriheten har mindre vekt enn normalt. Det finnes etter utvalgets undersøkelser videre ingen eksempler fra Høyesteretts praksis på at ytringer av den art som reguleres av tilleggsprotokollens artikkel 6 (1) har blitt rammet av straffeloven § 135 a. I Rt. 1977 side 114 ble domfellelsen av en lektor etter § 135 a opprettholdt av Høyesterett. Domfelte hadde i et avisintervju blant annet henvist til en fransk historiker som i sitt arbeid hadde sådd tvil om bruken av gasskamre under 2. verdenskrig, og herunder uttalt at historikerens undersøkelser fremsto som svært troverdige. Påtalemyndigheten hadde for lagmannsretten imidlertid ikke hevdet at tiltalte skulle straffedømmes for å ha ment at tyske nazister ikke nyttet gasskamre i utryddelsen av jøder. For dette forhold ble domfelte da heller ikke kjent skyldig i lagmannsretten. Domfellelsen var knyttet til andre uttalelser i avisintervjuet, blant annet at jøder i Norge burde emigrere eller isoleres i egne jødiske lokalsamfunn. Disse uttalelsene falt etter rettens vurdering inn under gjerningsbeskrivelsen i § 135 a.

### *Behovet for endringer i nasjonal rett*

Utvalget har kommet til at straffeloven § 135 a ikke dekker minimumsforpliktelsene nedfelt i tilleggsprotokollens artikkel 6 nr. 1 selv om bestemmelsen trolig kan anvendes i enkelte tilfeller. Spørsmålet blir derfor om straffeloven bør presiseres, slik at den utrykkelig vil ramme fornektelse, vesentlig minimalisering, aksept eller forsvar av folkemord eller forbrytelser mot menneskeheten.

Ytringsfriheten er i norsk rettstradisjon sterkt vernet gjennom Grunnloven § 100 og begrensninger i friheten må etter grunnlovsbestemmelsens andre ledd bygge på «særlig tungtveiende Hensyn». Straffeloven § 135 a og §§ 246 flg. representerer slike begrensninger i norsk rett og kan etter en konkret vurdering tale for en innskrenkning av ytringsfriheten. Det fremstår imidlertid etter utvalgets syn som tvilsomt om forbud mot ytringer om historiske begivenheter kan forsvares etter Grunnloven § 100 andre ledd. Et forbud vil etter utvalgets syn føre til en lovfesting av en bestemt sannhet og effektivt hindre at det fremmes kritiske ytringer mot denne sannhet. Ytringer som er positivt uriktige og som samfunnet tar avstand fra er også vernet etter Grunnloven § 100.

Utvalget er av den generelle oppfatning at det som i dag faller utenfor det straffbare området, av hensyn til det grunnleggende prinsippet om ytringsfrihet, heller ikke bør underlegges straffansvar. Utvalget tiltrer i denne sammenheng uttalelsene fra Ytringsfrihetskommisjonen i NOU 1999: 27, kapittel 6.3.3.4, som er gjengitt i kapittel 7.2 her.

Den sterke forankringen av ytringsfrihet og åpenhet i norsk rettstradisjon skiller seg etter utvalgets syn fra tilsvarende regulering i flere andre land. At visse land begrenser ytringsfriheten når ytringene er knyttet til hendelsene under 2. verdenskrig, må også ses på bakgrunn av disse landenes deltakelse i krigen. Utvalget er også av den oppfatning at et forbud mot å ytre seg om historiske begivenheter faktisk kan forsterke den skadelige virkning av ytringen ved at debatten flyttes fra det offentlige rom til «skjulte miljøer». En slik undertrykkelse av samfunnsdebatten vil åpenbart kunne føre til at motargumentene ikke kommer frem i like stor grad. Det anses videre sannsynlig at strafforfølgning av personer som har fremsatt de aktuelle ytringene vil kunne føre til at disse personene gjøres til «martyrer» i visse miljøer. Dette vil også kunne bidra til å styrke ytringenes påvirkningskraft i negativ retning.

Utvalget har etter dette kommet til at Norge bør benytte reservasjonsadgangen i tilleggsprotokollens artikkel 6 nr. 2 bokstav b. Hensynet til nordisk rettsenhet underbygger etter utvalgets vurdering denne løsningen. Det svenske lovutvalget som vurderte behovet for endringer i svensk rett, har som nevnt gått inn for å benytte reservasjonsretten etter tilleggsprotokollens artikkel 6 nr. 2 bokstav b, og Danmark har faktisk benyttet den samme reservasjonsadgangen ved ratifiseringen av protokollen.

Løsningen underbygges også av tilleggsprotokollens fortale, der det klart fremgår at protokollen ikke er ment å gi innvirkning på etablerte ytringsfrihetsprinsipper i nasjonal rett. Norge har som tidligere påpekt, sterke ytringsfrihetstradisjoner og verner trolig ytringer av den karakter som reguleres i tilleggsprotokollens artikkel 6. Dette gjelder i utgangspunktet også positivt feilaktige og støtende ytringer om de aktuelle historiske begivenheter.

*Alternative forslag*

Datakrimutvalgets mandat av 6. september 2005 fastsetter at der

> «tilleggsprotokollen åpner for at statene kan reservere seg, skal utvalget dessuten vurdere om reservasjonsadgangen bør benyttes, jf. artiklene 3, 5 og 6. Selv om utvalget eventuelt går inn for at reservasjonsadgangen bør benyttes, skal utvalget likevel fremme forslag om hvordan protokollen kan gjennomføres i norsk rett uten at det gjøres bruk av reservasjonsadgangen».

Utvalget har kommet til at Norge bør benytte reservasjonsadgangen i artikkel 6 nr. 2 bokstav b. Hvis norske myndigheter likevel velger å implementere bestemmelsen, kan dette etter utvalgets syn skje ved endring av straffeloven § 135 a, eller ved å gi et helt nytt straffebud som implementerer gjerningsbeskrivelsen i artikkel 6 nr. 1. Utvalget er av den oppfatning at en endring av straffeloven § 135 a, ikke er tilrådelig i foreliggende sammenheng. Endringene i den eksisterende bestemmelsen trådte i kraft 1. januar 2006 og ytterligere endringer vil på det nåværende tidspunkt kunne medføre rettslig usikkerhet. Det er videre på det rene at skyldkravet etter tilleggsprotokollens artikkel 6 er forsett, mens straffeloven § 135 a også rammer grov uaktsomhet. Henvisningen til internasjonal rett og praksis i artikkel 6 underbygger videre denne løsningen all den tid § 135 a ikke inneholder tilsvarende henvisning. Straffeloven § 135 a skal som nevnt fortolkes i samsvar med den grunnlovsvernede ytringsfrihet, og terskelen for inngrep etter § 135 a er etter rettspraksis høy. Straffeloven § 135 a rammer videre som nevnt ytringer som truer, forhåner, fremmer hat, forfølgelse eller ringeakt overfor noen, mens artikkel 6 nr. 1 ikke stiller opp tilsvarende vilkår.

Hvis Norge ikke velger å benytte reservasjonsadgangen etter tilleggsprotokollens artikkel 6 nr. 2 bokstav b, foreslår utvalget derfor en selvstendig straffebestemmelse som kan gis følgende ordlyd:

> «Fornektelse, vesentlig minimalisering, aksept eller forsvar av folkemord eller andre forbrytelser mot menneskeheten.
>
> For krenkende ytring straffes den som setter frem offentlig en ytring som fornekter, vesentlig minimaliserer, aksepterer eller forsvarer folkemord eller andre forbrytelser mot menneskeheten. Likt med en offentlig fremsatt ytring, jf. § 10 annet ledd regnes en ytring når den er satt frem slik at den er egnet til å nå et større antall personer.
>
> Med folkemord og forbrytelser mot menneskeheten menes handlinger som i internasjonal rett og praksis fra anerkjente internasjonale domstoler, er klassifisert som forbrytelser.
>
> Straffen er bøter eller fengsel inntil 3 år.»

Utvalget viser i denne sammenheng til straffenivået i straffeloven § 135 a, som kan tjene som en hensiktsmessig parallell her. Det vises videre til definisjonen av «offentlig sted» i den nye straffeloven § 10 annet ledd.

### 7.4.6 Medvirkning – artikkel 7

Artikkel 7 regulerer medvirkning til lovbrudd etter tilleggsprotokollen og fastsetter følgende:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminaloffences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.»

Bestemmelsen pålegger medlemslandene å straffbelegge medvirkning til ethvert lovbrudd som reguleres i tilleggsprotokollens artikkel 3-6. Utvalget har i kapittel 7.4.1 påpekt at kravet om subjektiv skyld etter tilleggsprotokollen beror på nasjonal lovgivning. Det følger imidlertid av den forklarende rapporten (side 8) at medvirkerens forsett må dekke gjennomføringen av hovedmannens straffbare handling.

Straffeloven § 135 a, første ledd og § 227 rammer utrykkelig medvirkningshandlinger og utvalget forutsetter følgelig at forpliktelsene etter artikkel 7 er dekket i tilknytning til de handlinger som er regulert i artikkel 3, 4 og 5. Utvalget har, som det fremgår i kapittel 7.3.5, imidlertid kommet til at Norge bør benytte reservasjonsadgangen etter artikkel 6, men har likevel foreslått et alternativt lovforslag. Det fremheves i denne sammenheng at medvirkning til overtredelser av dette straffebudet vil være straffbart etter den nye straffeloven § 15 når denne trer i kraft. Forpliktelsene etter tilleggsprotokollens artikkel 7, jf. artikkel 6, anses derfor ivaretatt ved § 15.

Utvalget fremhever videre at forsøk på straffbare handlinger ikke rammes av tilleggsprotokollen. Dette fremgår utrykkelig av den forklarende rapporten (side 8) og begrunnes med at flere av de straffbare handlinger som reguleres i tilleggsprotokollen i seg selv er av forberedende karakter. Tilleggsprotokollen skiller seg således fra selve datakrimkonvensjonen på dette punkt. Utvalget presiserer videre at forsøk på overtredelse av straffelo-

ven §§ 135 a og 227 er straffbare etter gjeldende straffelov § 49, og ny straffelov § 16. Norsk rett går følgelig lengre enn det som kreves etter tilleggsprotokollen.

## 7.5 Forholdet mellom konvensjonen og tilleggsprotokollen – kapittel III

### 7.5.1 Forholdet mellom konvensjonen og tilleggsprotokollen – artikkel 8

Tilleggsprotokollen artikkel 8 regulerer den nærmere bestemte sammenhengen mellom datakrimkonvensjonen og tilleggsprotokollen og fastsetter det følgende:

«1. Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, mutatis mutandis, to this Protocol.
2. The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.»

Tilleggsprotokollen artikkel 8 fastsetter spesifikt hvilke bestemmelser i datakrimkonvensjonen som gis anvendelse på tilleggsprotokollens område.

## 7.6 Avsluttende bestemmelser – kapittel IV

Artiklene nedfelt i tilleggsprotokollens kapittel IV er standardklausuler som benyttes i Europarådets konvensjoner, og utvalget finner det derfor ikke påkrevd å kommentere disse. Det er imidlertid på det rene at noen av standardklausulene er modifiserte i tilknytning til tilleggsprotokollen og disse kommenteres i det følgende.

Artikkel 12 nr. 2 fastsetter at medlemslandene kan benytte reservasjonsretten nedfelt i artiklene 3, 5 og 6. Bestemmelsen fastsetter deretter uttømmende i hvilken grad det enkelte medlemsland kan benytte reservasjonsretten.

Det fremgår av artiklene 9 og 10 at tilleggsprotokollen kun kan signeres av medlemsland som er signerende parter under datakrimkonvensjonen. Tilleggsprotokollen vil videre tre i kraft 3 måneder etter at fem signerende parter til datakrimkonvensjonen har samtykket til å bli bundet av tilleggsprotokollen.

# Kapittel 8
# Jurisdiksjon - Straffelovens stedlige virkeområde

## 8.1 Innledning

Datakriminalitet reiser spørsmål knyttet til jurisdiksjon. Det er særlig datakriminalitetens internasjonale og grenseløse karakter som får betydning både i forhold til spørsmålet om hvor en handling skal anses begått og hvorvidt vedkommende skal kunne strafforfølges i Norge.

## 8.2 Folkerettslige forpliktelser

Datakrimkonvensjonen artikkel 22 regulerer jurisdiksjon og lyder:

«1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å etablere jurisdiksjon med hensyn til enhver straffbar handling fastslått i samsvar med artikkel 2 til 11 i denne konvensjon, når den straffbare handlingen er begått:
   a) på denne partens territorium, eller
   b) om bord på et skip som fører denne partens flagg, eller
   c) om bord på et luftfartøy som er registrert etter denne partens rett, eller
   d) av en borger av denne part dersom handlingen kan straffes på det sted handlingen ble begått, eller dersom den straffbare handlingen er begått utenfor enhver stats territoriale jurisdiksjon.
2. Hver stat kan forbeholde seg retten til ikke å anvende eller til bare å anvende i bestemte tilfeller eller på bestemte vilkår reglene om jurisdiksjon fastsatt i nr. 1 b) til d) i denne artikkel eller deler av disse.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå jurisdiksjon med hensyn til de straffbare handlingene omhandlet i artikkel 24 nr. 1 i denne konvensjon, når den antatte gjerningsmann befinner seg på partens territorium og parten ikke utleverer vedkommende til en annen part utelukkende av hensyn til vedkommendes nasjonalitet, etter en anmodning om utlevering.
4. Denne konvensjon utelukker ikke straffe-rettslig jurisdiksjon som utøves i samsvar med nasjonal rett.
5. Når mer enn en part gjør krav på jurisdiksjon med hensyn til en påstått straffbar handling fastslått i samsvar med denne konvensjon, skal de berørte parter, når det er hensiktsmessig, rådføre seg med hverandre for å bestemme hvilken jurisdiksjon som er best egnet til å gjennomføre rettsforfølgningen.»

Artikkel 22 oppstiller krav til det stedlige virkeområdet til straffebud som er nevnt i konvensjonen artikkel 2 til 11.

Artikkel 22 nr. 1 bokstav a forplikter statene til å gjennomføre territorialprinsippet. Dette innebærer at statene skal kunne strafforfølge handlinger som er begått på statens eget territorium. En handling anses å være begått innenfor statens territorium når gjerningspersonen og objektet for den straffbare handlingen (for eksempel datasystemet) befinner seg der. Det samme gjelder når hele eller deler av det datasystemet som berøres av den straffbare handlingen er plassert i territoriet selv om gjerningspersonen selv ikke befinner seg der, jf. den forklarende rapporten punkt 233.

Etter artikkel 22 nr. 1 bokstav b skal statene også kunne strafforfølge handlinger som begås på skip som seiler under statens flagg. Det samme gjelder etter artikkel 22 nr. 1 bokstav c for handlinger som begås på luftfartøy som er registrert i henhold til statens lover. Etter artikkel 22 nr. 1 bokstav d skal statene også kunne strafforfølge handlinger som begås i utlandet av egne statsborgere forutsatt at handlingen også var straffbar i landet hvor den ble begått, eller dersom handlingen ikke ble begått innenfor territoriet til en stat.

Statene er i artikkel 22 nr. 2 gitt adgang til å reservere seg mot å gjennomføre artikkel 22 nr. 1 bokstav b til d.

Artikkel 22 nr. 3 forplikter statene til å gjennomføre prinsippet «extradite or prosecute» (utlevering eller straffeforfølgning). Prinsippet innebærer at dersom en stat nekter å utlevere egen borger etter å ha mottatt en begjæring om det i henhold til artikkel 24 nr. 1, plikter staten selv å strafforfølge vedkommende dersom handlingen er straffbar etter nasjonal rett.

Bestemmelsene i artikkel 22 er ikke til hinder for at statene etablerer en mer vidtrekkende jurisdiksjon enn det som følger av konvensjonen, jf. artikkel 22 nr. 4.

Etter artikkel 22 nr. 5 skal statene, såfremt det er hensiktsmessig, konsultere hverandre når en straffbar handling får virkning i flere stater. Dersom en handling etter omstendighetene dekkes av flere staters jurisdiksjon, skal statene så langt det er hensiktsmessig konsultere hverandre om hvor handlingen skal strafforfølges.

## 8.3 Kort om gjeldende rett – straffeloven § 12

Det følger av straffeloven § 12 første ledd nr. 1 at norsk straffelov får anvendelse på handlinger som er foretatt i riket (territorialprinsippet). Når det gjelder forståelsen av begrepet «i riket» vises det til Ruud/Ulfstein «Innføring i folkerett» kapittel 7. Det vises også til redegjørelsen for gjeldende rett i Ot.prp. nr. 90 (2003-2004) side 176-178. Straffeloven er gitt anvendelse på norske skip og luftfartøy som befinner seg utenfor territorialgrensen, jf. § 12, første ledd nr. 1 bokstav d og e.

Av straffeloven § 12 første ledd nr. 3 følger det at norske statsborgere i visse tilfeller kan strafforfølges i Norge for handlinger de har begått i utlandet (nasjonalitetsprinsippet). Hva som regnes som «utlandet» innbefatter alle områder som etter § 12 første ledd nr. 1 og 2 ikke regnes som «riket». Etter bestemmelsen kan blant annet norske borgere strafforfølges for handlinger foretatt i utlandet når vilkårene i straffeloven § 12 første ledd nr. 3 er til stede. Ved lov av 8. april 2005 ble det gjort en endring i § 12 første ledd nr. 3 for å bringe bestemmelsen i samsvar med konvensjonen. Opplistingen i § 12 første ledd nr. 3 fikk med lovendringen tilføyd en henvisning til § 145 annet ledd og § 145 b.

Etter straffeloven § 12 første ledd nr. 4 er det også adgang til å strafforfølge utlending for forbrytelse begått i utlandet, jf. vilkårene avgitt i nr. 4 bokstav a-d. Bestemmelsen gir mulighet for å straffe datakriminalitet begått av utlending i utlandet, dersom handlingen er straffbar både etter norsk lov og etter dets lands lov hvor handlingen ble begått, jf. bestemmelsens punkt b.

Straffeloven § 12 annet ledd bestemmer at hvor en handlings straffbarhet avhenger eller påvirkes av en inntrådt eller tilstiktet virkning, betraktes handlingen som foretatt også der hvor virkningen er inntrådt eller tilsiktet fremkalt. Det antas at bestemmelsen kan ha betydning for datakriminalitet som skjer på internett m.v. som typisk karakteriseres ved at gjerningspersonen benytter en datamaskin i ett land til å skape en effekt på et datasystem i et annet land. Regelen kan være aktuell der gjerningspersonen er i utlandet mens virkningen har inntrådt i Norge. Spørsmålet er nærmere drøftet i kapittel 8.4.4.

## 8.4 Utvalgets vurderinger

I NOU 2003: 27 «Lovtiltak mot datakriminalitet» (Delutredning I) ble gjeldende rett vurdert mot utvalgets daværende mandat. Datakrimutvalgets arbeid resulterte blant annet i endringen i § 12 første ledd nr. 3 som nevnt ovenfor i kapittel 8.3. Datakrimutvalget har denne gang hatt et videre mandat vedrørende regulering av datakriminalitet og må vurdere om gjeldende rett og de vedtatte endringer i ny straffelovs alminnelige del vil gi en tilstrekkelig jurisdiksjon for de endringene i straffelovgivningen som utvalget nå foreslår under det nye mandatet.

### 8.4.1 Handlinger som er begått i Norge og på norske jurisdiksjonsområder

I NOU 2003: 27 ble det konkludert med at straffeloven § 12 første ledd nr. 1 dekker konvensjonens forpliktelser for så vidt gjelder handlinger begått på norsk territorium samt handlinger som er begått på om bord på norsk skip eller luftfartøy, jf. artikkel 22 nr. 1 bokstav a til c. I den nye straffeloven er dette etter utvalgets vurdering ivaretatt på en dekkende måte i § 4 som i det alt vesentlige representerer en videreføring av gjeldende straffeloven § 12 første ledd nr. 1 og 2, dog med noen endringer, blant annet hva gjelder norsk strafferettslig jurisdiksjon i maritime soner som er regulert i ny straffelov § 4 annet ledd bokstav b, se Ot.prp. nr. 90 (2003-2004) side 399-401.

Datakriminalitetens ofte internasjonale preg kan innebære at handlinger begås på tvers av landegrenser og i samvirke mellom personer i ulike land til samme tid. Det kan også være vanskelig å fastslå i hvilket land den straffbare handlingen er begått. Det er viktig å sikre at nordmenn kan strafforfølges i Norge da norske borgere etter utleveringsloven (lov av 13. juni 1975 nr. 39) § 2 ikke kan utleveres til land utenfor Norden. I henhold til artikkel 22 nr. 3 er statene forpliktet til å gjennomføre prinsippet «extradite or prosecute». Prinsippet innebærer som tidligere nevnt at dersom en stat nekter å utlevere egen borger etter å ha mottatt

begjæring om det etter artikkel 22 nr. 3, plikter staten selv å strafforfølge vedkommende dersom handlingen er straffbar etter norsk rett.

Det internasjonale preget ved datakriminalitet er særlig synlig ved for eksempel generelle dataangrep. Disse kjennetegnes ved at de ikke er målrettet, men er rettet mot dataressurser der de er tilgjengelige og er således uten noen naturlig geografisk avgrensning. Spørsmålet om straffelovens stedlige virkeområde kom på spissen i Rt. 2004 side 1619 (bakdørkjennelsen). Her avgjorde Høyesterett at norsk rett får anvendelse i en sak hvor handlingen var rettet mot datamaskiner som befant seg i utlandet, men hvor alle nødvendige handlinger for å overtre straffebudet var foretatt i Norge.

Saken gjaldt to personer som hadde begått datainnbrudd og skadeverk på i alt 437 servere verden over. I forhold til straffeloven § 145 annet ledd og ett tilfelle av overtredelse av § 393 ble det anført at handlingene var straffrie fordi de ikke kunne anses begått i riket, jf. straffeloven § 12 første ledd nr. 1. Verken § 145 annet ledd eller straffeloven § 393 var på det tidspunkt inntatt i opplistingen i straffeloven § 12 første ledd nr. 3 bokstav a. Høyesterett kom i likhet med de foregående instanser til at handlingen var begått i riket og kunne straffes. Det vesentlige var at:

> «de datamaskiner de tiltalte brukte og de fysiske handlingene, kommandoene, som iverksatte søk mot og inntregning i de andre datamaskinene, var i riket. Uten den handlingen og utstyret i riket, faller også resten av handlingsrekken bort.» (Rt. 2004 side 1619 avsnitt 17)

Når det gjelder datakriminalitet og hva som skal til for at en handling kan anses inntruffet i Norge, vises det også til RG 2001 side 219 som gjelder publisering av nettsider med ulovlig innhold. I denne saken gjaldt det nettsider med pornografisk innhold. Denne problemstillingen er behandlet særskilt nedenfor i kapittel 8.5.

### 8.4.2 Handling som er foretatt utenfor noen stats høyhetsrett

I Datakrimutvalgets delutredning I ble det stilt spørsmål om gjeldende rett ga hjemmel for å strafforfølge norske borgere for handlinger begått i områder som ikke er underlagt noen stats territorialhøyhet, jf. artikkel 22 nr. 1 bokstav d. Usikkerheten knyttet til anvendelsen av rekkevidden for straffeloven § 12 annet ledd som kan anvendes dersom virkningen av en handling er inntrådt eller tiltenkt inntrådt i Norge, samt hensynet til å sikre en lojal etterlevelse av konvensjonsteksten, ble benyttet som argument for at Norge burde vurdere en lovendring her med mindre man valgte å benytte reservasjonsadgangen i artikkel 22 nr. 2.

I den nye straffelovens alminnelig del er dette nå i forhold til konvensjonens krav, i tilstrekkelig grad ivaretatt i § 5 første ledd nr. 7. Etter denne bestemmelsen gjelder straffelovgivningen for handlinger foretatt av en norsk statsborger, en person med bosted i Norge eller på vegne av et foretak registrert i Norge når den er «foretatt utenfor området for noen stats høyhetsrett og kan straffes med fengsel». Bestemmelsen er ny i forhold til gjeldende lov, men elementet av nykriminalisering blir i forarbeidene til ny straffelovs alminnelige del i Ot.prp. nr. 90 (2003-2004) side 403 ansett å være begrenset. Dette skyldes at en rekke overtredelser av gjeldende straffelov anses å være straffbare i Norge etter § 12 første ledd bokstav a også når de er forøvet utenfor områder hvor noen land har overhøyhet. Bestemmelsen er også i samsvar med forslag fra Nordisk strafferettskomité.

### 8.4.3 Handling begått i utlandet av en utlending

I NOU 2003: 27 side 52 ble det ikke foreslått å utvide norsk jurisdiksjon til også å omfatte handlinger begått i utlandet av en utlending. Dette er heller ikke noe krav som konvensjonen i alminnelighet oppstiller. I konvensjonens artikkel 22 nr. 3 er det imidlertid forutsatt at slike bestemmelser må innføres dersom gjerningspersonen befinner seg på statens territorium og myndighetene beslutter å ikke utlevere vedkommende utelukkende av hensyn til vedkommendes nasjonalitet etter en anmodning om utlevering etter artikkel 24 nr. 1. Det er vanskelig å tenke seg en situasjon hvor den norske stat nekter å etterkomme en slik utleveringsanmodning fra et medlemsland. Heller ikke i denne omgang har utvalget har funnet det nødvendig å foreslå en endring av rettstilstanden på dette punktet.

Den motsatte situasjonen enn den som forelå i bakdørkjennelsen i Rt. 2004 side 1619, foreligger hvor datasystem i Norge angripes fra utlandet. Dersom gjeldende rett i det aktuelle land hvor angrepet kommer fra gir grunnlag for samme resultat som den i «bakdørkjennelsen», vil handlingen anses som å ha funnet sted i det aktuelle land, og straffeforfølgning vil kunne skje der med mindre det finner sted en utlevering til Norge.

I følge den forklarende rapporten punkt 233 vil imidlertid handlingen også anses å ha funnet sted

her dersom hele eller deler av det datasystemet som berøres av den straffbare handlingen er plassert i territoriet selv om gjerningspersonen selv ikke befinner seg der, jf. den forklarende rapporten punkt 233.

Det antas også at § 12 andre ledd som gjelder handling som anses foretatt på flere steder i noen tilfeller vil utvide norsk jurisdiksjon utover de tilfeller som er beskrevet ovenfor. § 12 andre ledd er videreført i den nye straffeloven § 7. Bestemmelsen er gitt en særskilt behandling nedenfor under kapittel 8.4.4.

### 8.4.4 Handling som anses foretatt på flere steder

Hensynet til andre lands suverenitet tilsier at det bør utvises varsomhet med å strafforfølge i Norge for handlinger som er begått på andre lands territorium. Folkerettslig vil det være aktuelt å anvende det såkalte «objektive territorialprinsipp» på overtredelser etter datakrimkapitlet. Se for øvrig Ian Brownlie «Principles of Public International Law», som omtaler prinsippet i punkt 3 om jurisdiksjon innen strafferetten under navnet «objective territorial principle». Prinsippet har vært anvendt på strafferettslige overtredelser som er initiert i ett territorium, men som får virkning på ett annen territorium. Denne type jurisdiksjon er i teorien ofte eksemplifisert ved et skudd som blir avfyrt fra et territorium, over landegrensen, for så å skade noen på et annet territorium. Det er allment akseptert at landet der skaden skjedde, kan straffe gjerningspersonen.

Av ny straffelov § 7 følger det at når straffbarheten av en handling avhenger eller påvirkes av en inntrådt eller en tilsiktet virkning, anses handlingen foretatt også der virkningen er inntrådt eller tilsiktet fremkalt. Bestemmelsen er en videreføring av den gjeldende bestemmelsen i straffeloven § 12 annet ledd.

I NOU 2003: 27 på side 52 anføres det at rekkevidden av straffeloven § 12 annet ledd er usikkert, og det vises i den forbindelse til den ovenfor nevnte avgjørelse i RG 2001 side 219 som gjaldt pornografisk materiale på internett. I denne avgjørelsen ble § 12 annet ledd tolket vidt ved at publisering på internett ble ansett tilstrekkelig til at innholdet hadde virkning i Norge etter § 12 annet ledd. Dette selv om hjemmesiden ikke fremstod som spesielt rettet mot et norsk publikum. Dette er imidlertid kun en underrettsavgjørelse med begrenset vekt.

I forarbeidene til den nye straffeloven alminnelige del er bestemmelsen grundig behandlet. Dersom en handling faller inn under bestemmelsen, skal handlingen anses begått begge steder. Straffelovkommisjonen overlot til et eget underutvalg å vurdere spørsmålet om straffelovens stedlige virkeområde. Underutvalget fremla sin utredning som Straffelovkommisjonens delutredning II, NOU 1984: 31. Som eksempel på tilfeller som faller inn under bestemmelsen, nevnes at en terrorist i Italia sender en brevbombe til en adressat i Norge. I 1984 var jurisdiksjonsutfordringen knyttet til internasjonal datakriminalitet av begrenset betydning. Mer overraskende er det at denne problemstillingen heller ikke behandles i senere forarbeider som for eksempel i Ot.prp. nr. 90 (2003-2004).

Det ene vilkåret i ny straffelov § 7 er at handlingen har virkninger som er avgjørende for eller påvirker straffbarheten. Det andre hovedvilkåret er at virkningen enten har inntrådt på territoriet, eller at det var innenfor lovbryterens forsett at virkningen skulle inntre på norsk territorium (tilsiktet).

På side 405 i Ot.prp. nr. 90 (2003-2004) fremkommer det at virkninger som er avgjørende eller som påvirker straffbarheten lettest kan tenkes ved fare- eller skadedelikter hvor utførelsen av selve den straffbare handling og resultatet av den ikke faller sammen verken i tid eller sted. Det anføres videre at det særlig for straffebud som gjør straffbarheten eller subsumsjonen avhengig av at en skade, et tap eller en fare har inntrådt, kan være aktuelt at virkningen har inntrådt i Norge, selv om handlingen er utført i utlandet. I Rt. 2003 side 1770 ble grovt bedrageri utført fra Sverige, Finland og Bahamas. Det falt klart innenfor lovbryterens forsett at de som skulle bedras primært befant seg i Norge. Et betydelig tap oppstod også i Norge. Dette var tilstrekkelig til å anse at handlingen også hadde handlingssted i Norge.

Felles for de fleste av utvalgets forslag til lovbestemmelser, er at de fastsetter straffbarhet for handlinger som begås via datasystem og elektronisk kommunikasjon og at dette er handlinger som kan begås uavhengig av geografiske grenser. Det beror imidlertid på en tolkning av det enkelte foreslåtte straffebud hvorvidt en handling i samsvar med straffebudet fyller vilkårene i ny straffelov § 7 slik at norsk rett kommer til anvendelse på handlingen.

Hvorvidt en handling som regulert i det foreslåtte kapitlet om datakriminalitet faller inn under norsk jurisdiksjon kan i det enkelte tilfelle fremstå som uklart. At rekkevidden av ny straffelov § 7, nåværende § 12 andre ledd, fremstår som usikker, hevdes som ovenfor nevnt også i NOU 2003: 27 på side 52. Utkastet § 13 om driftshindring som igangsettes fra utlandet mot norske datasystem har for

eksempel åpenbart en konsekvens for den som rammes i Norge. Identitetstyveri etter kapittel 15 gjennom elektronisk kommunikasjon med mottaker i Norge, kan medføre at mottaker blir villedet og derigjennom kan komme til å lide et tap. Det er imidlertid noe usikkert hvorvidt de foreslåtte straffebud kan betegnes som følge- eller skadedelikt.

Selv om det ikke er noe absolutt krav om at et straffebud må være et følge- eller skadedelikt for at den nye straffeloven § 7 kommer til anvendelse, synes rettstilstanden noe uoversiktlig og lite forutberegnelig. Utvalget mener også at det er unødvendig tungvint at rettstilstanden skal måtte utledes av usikre tolkninger og rettspraksis. Utvalget foreslår derfor et tillegg til ny straffelov § 7 for å avklare rettstilstanden på området. I henhold til den foreslåtte bestemmelsen, skal virkningen av en handling anses inntrådt etter § 7, første punktum når et datasystem eller elektronisk kommunikasjonsnett i Norge er rammet eller forsøkt rammet. Se nedenfor under kapittel 8.6.

## 8.5 Jurisdiksjonsspørsmålet vedrørende ulovlig materiale på internett

Utvalget ble bedt om å særlig vurdere om straffelovens stedlige virkeområde i den nye straffeloven alminnelige del innebærer hensiktsmessige avgrensninger når det gjelder ulovlig materiale på internett. Det sentrale er å avgjøre hvor langt norske myndigheter kan og bør gå for å bekjempe ulovlig materiale på nettet.

En av de internasjonalt mest kjente sakene som gjelder jurisdiksjonsspørsmålet ved publisering av ulovlig materiale på internett, er den såkalte Yahoo-saken. Det amerikanske selskapet Yahoo avholdt på sine sider auksjoner for salg av Naziutstyr, hvilket var ulovlig i Frankrike, mens det var lovlig i USA. Selskapet var som nevnt amerikansk og serveren selskapet benyttet lå heller ikke i Frankrike. Yahoo ble imidlertid saksøkt i Frankrike hvor selskapet ble dømt til å hindre franske nettbrukere adgang til disse auksjonene. Retten mente at siden ble rammet av fransk lov når den var tilgjengelig for franske nettbrukere i Frankrike. Siden var dessuten spesielt tilrettelagt for franske brukere ved at den blant annet var utformet på fransk. Yahoo ble ikke hørt med sine påstander om at de ikke kunne filtrere ut nettbrukere i Frankrike. Den oppmerksomhet og det press Yahoo ble gjenstand for i forbindelse med saken, har ført til at Yahoo senere har innført et generelt forbud mot å tillate auksjoner for lignende effekter på sine sider. Saken er utføring omtalt i Schwaback «Internet and the Law» side 157-160.

En annen sak som har blitt viet mye oppmerksomhet internasjonalt, er Dow Jones & Co v Gutnick. The High Court of Australia tok jurisdiksjon i en sak om ærekrenkelse hvor teksten lå på en server i USA. Den australske domstolen la til grunn at for materiale publisert på internett var forholdet begått på det stedet hvor ærekrenkelsen var oppstått – og det var der hvor nettsiden ble lastet ned. Saken er utførlig omtalt i Goldsmith og Wu «Who Controls the Internet?» side 147-148 og side 156-161.

De to ovennevnte avgjørelser er omdiskutert internasjonalt.

I den tidligere refererte dommen fra RG 2001 side 219 som gjaldt publisering av pornografisk materiale på internett, kom herredsretten til at handlingen falt innenfor norsk jurisdiksjon på to ulike grunnlag. Handlingen ble ansett begått i riket i henhold til straffeloven § 12 første ledd. I denne saken befant gjerningspersonene seg i Norge og filene var også lastet opp i Norge. Det eneste som skjedde via en utenlandsk server, var kjøp av lagringsplass samt selve distribusjonen. Forholdet ble samtidig funnet å falle inn under § 12 andre ledd fordi virkningen hadde inntrådt i Norge. Dette er som nevnt en underrettsavgjørelse og retten tilrår i dommen at de rettslige konsekvenser ved bruk av servere i utlandet undergis en nærmere utredning og avklaring.

Når det gjelder handlinger som utføres av personer som befinner seg i Norge mot datasystem i utlandet, fikk man en avklaring med den ovennevnte bakdørkjennelsen i Rt. 2004 side 1619, hvor Høyesterett avgjorde at norsk rett får anvendelse hvor handlingen var rettet mot datamaskiner som befant seg i utlandet, men hvor alle nødvendige handlinger for å overtre straffebudet var foretatt i Norge.

Spørsmålet er hvor langt norsk jurisdiksjon gjelder for – eller bør gjelde for – nettsider med materiale som er straffbart etter norsk lov som er publisert av utlendinger i utlandet.

I avgjørelsen i RG 2001 side 219 kom retten til at nettsiden fikk virkning i Norge ved å være publisert på internett og således være tilgjengelig fra Norge. Dette er en vid tolkning av lovens krav om at virkningen av handlingen skal ha inntrådt her. Som underrettsavgjørelse har dommen begrenset vekt. Alternativet hadde vært at retten tolket inn et krav om at det må noe mer til for at siden skulle anses for å ha virkning i Norge, for eksempel at siden var på norsk. Det er grunn til å bemerke at sidene var laget av nordmenn i Norge. Det var da

unødvendig av retten å ta standpunkt til dette spørsmålet siden den også kom til at handlingen var å anse som «begått i riket», jf. straffeloven § 12 første ledd nr. 1.

Hensynet til andre lands suverenitet tilsier som nevnt at det bør utvises varsomhet med å strafforfølge i Norge for handlinger som er begått på andre lands territorium. Etter utvalgets mening, er man heller ikke tjent med regler som gjør enhver nettside publisert i utlandet straffbar i ethvert land hvis lovgivning den er i strid med. Ved etablering av en nettside vil det være umulig å ha full kunnskap om hvorvidt innholdet vil være straffbart etter noe lands lovgivning. Det vil bli svært vanskelig å publisere noe dersom man må ta hensyn til alle ulike lands jurisdiksjon. Konsekvensen vil da også være at det blir det land med den strengeste lovgivningen som vil sette den rettslige standarden til enhver tid.

I normaltilfellene hvor en nettside er laget av utlendinger i utlandet og publisert på en utenlandsk server, vil dette falle utenfor norsk jurisdiksjon. Unntak fra dette utgangspunktet kan tenkes dersom det for eksempel er tale om nettsider som er spesielt tilrettelagt for bruk i Norge og hvor de negative konsekvensene i hovedsak eller utelukkende manifesterer seg her. Et eksempel er nettsteder med spilltjenester som markedsføres direkte mot det norske markedet for eksempel ved at nettstedet har norsk tekst. Dette vil da kunne anses som kriminalitet som er begått i utlandet, men som får virkning i Norge og må derfor kunne straffes her hvor virkningen inntrer. Hvorvidt en nettside med ulovlig innhold vil kunne rammes av norsk rett, vil bero på en tolkning av om vilkårene i ny straffelov § 7 er oppfylt i det konkrete tilfellet.

De generelle reglene om jurisdiksjon som er omtalt ovenfor kan i enkelte tilfeller tenkes å komme i konflikt med konkrete bestemmelser i traktater som Norge er bundet av. I slike tilfeller følger det av § 2 i ny straffelov at folkerettslige forpliktelser går foran jurisdiksjonsbestemmelsene. I tillegg inneholder EØS-loven generelle regler om forrang for lov og forskrift som er gitt for å gjennomføre forpliktelser etter EØS-avtalen.

EUs någjeldende tv-direktiv (direktiv 89/552/EØF, endret ved direktiv 97/36/EF) har som hovedregel at det er sendelandets rett som følges når det gjelder innholdet i sendingene. Det gjelder en rekke unntak fra denne hovedregelen. Dette direktivet er omfattet av EØS-avtalen, og således folkerettslig bindende for Norge. Direktivet er også gjennomført i norsk rett. Det er foreslått ytterligere reguleringer i forslag til endring i direktiv 89/552/EØF som er fremlagt som forslag 2005/0260 (COD).

Konvergens mellom ulik teknologi og medier, gjør direktivet også relevant for andre innholdstjenester enn tv-tjenester, blant annet for internettjenester. EU-Kommisjonen ønsker ikke at reguleringen skal forskjellsbehandle ulike teknologiske plattformer som leverer lignende innhold. Endringsforslaget innebærer derfor bl.a. en utvidelse av virkeområdet til alle typer audiovisuelle medietjenester uansett hvilken plattform de leveres fra. Det skal være en gradert regulering basert på en sondring mellom lineære (for eksempel tradisjonell kringkasting) og ikke-lineære tjenester (for eksempel on-demand-tjenester). Utvalget legger til grunn at forslaget til endringer i direktiv 89/552/EØF vil være EØS-relevant og vil bli vurdert for innlemming i EØS-avtalen i samsvar med vanlig prosedyre.

## 8.6 Utvalgets forslag

På bakgrunn av redegjørelsen ovenfor, foreslår utvalget en endring i ny straffelov § 7 som presiserer rettstilstanden for hvor en handling under kapitlet om datakriminalitet skal anses å ha funnet sted. Utvalget foreslår tilføyelse av ny setning i § 7, som dermed vil lyde:

§ 7 Handling som anses foretatt på flere steder

Når straffbarheten av en handling avhenger eller påvirkes av en inntrådt eller tilsiktet virkning, anses handlingen foretatt også der virkningen er inntrådt eller tilsiktet fremkalt.

*Er et datasystem eller elektronisk kommunikasjonsnett i Norge rammet eller forsøkt rammet av en handling som er straffbar etter kapitlet om «Vern av data, databasert informasjon og datasystemer», anses virkningen inntrådt i Norge.*

Når det gjelder § 7 første punktum vises det til de øvrige forarbeidene til denne bestemmelsen, blant annet i spesialmotivene til § 7 i Ot.prp. nr. 90 side 405-406.

Formålet med det nye foreslåtte andre punktum, er å fjerne usikkerhet med hensyn til rekkevidden av norsk jurisdiksjon når det gjelder brudd på straffebestemmelser i datakrimkapitlet fra utlandet når datasystem eller elektronisk kommunikasjonsnett i Norge er rammet eller forsøkt rammet. I slike tilfeller er det ikke nødvendig å gå veien om en tolkning av om en virkning er «inntrådt» eller «tilsiktet fremkalt» i Norge. Dersom datasystemer i Norge er rammet eller forsøkt rammet, vil virkningen etter annet ledd automatisk bli

ansett for å ha inntrådt i Norge. For begrepene «datasystem» og «elektronisk kommunikasjonsnett» vises det til utkastet § 1 bokstav a og e og kapittel 5.2 og 9.1.

Ny straffelov § 7 første punktum omfatter i utgangspunktet kun fullbyrdede handlinger. Utvalget har imidlertid valgt å la forsøk være straffbart etter annet punktum. Dette skyldes blant annet arten og alvorligheten av de handlinger som rammes av datakrimkapitlet. Det kan påbegynnes handlinger med omfattende skadepotensiale som av en eller annen grunn, tilfeldig eller som på grunn av sikkerhetstiltak, blir avverget før fullbyrdelsen. Slike forsøkshandlinger på dette området er etter utvalgets oppfatning så straffverdig at også slike bør være straffbare.

## 8.7 Sammenhengen mellom jurisdiksjonsregler og faktisk adgang til strafforfølgning

Selv om en handling i utgangspunktet omfattes av norsk jurisdiksjon, innebærer ikke dette nødvendigvis en faktisk adgang til straffeforfølgning. Dette avhenger av grunnleggende bestemmelser i straffeprosesslovgivningen om rettens mulighet til å få forkynt varsler, fremtvinge tilstedeværelse, foreta avhør, samt øvrige rettergangsskritt.

Datakrimkonvensjonen har sine begrensninger. Foreløpig har kun et begrenset antall land gjennomført den, og hensynet til den enkelte stats suverenitet legger begrensninger på for eksempel mulighetene for etterforskningsskritt på tvers av landegrensene.

Goldsmith og Wu: «Who controls the Internet? Illusions of a borderless world» side 163-165 beskriver en illustrerende sak hvor en person i Chelyabinsk i Russland brøt seg inn på servere tilhørende amerikanske selskap. Etter å ha brutt seg inn på serverne, kontaktet han selskapene på vegne av en gruppe han kalte: » The Expert Group of Protection Against Hackers» med krav om betydelige beløp mot å få kunnskap om hvordan sikkerhetshullene kunne tettes. Dersom et selskap ikke gikk med på dette, ville de risikere at filer ble slettet eller at kunders kredittkortinformasjon ble tilgjengeliggjort på nettet.

Da FBI skulle etterforske saken, ga de seg ut for å være et amerikansk sikkerhetsselskap og inviterte hackeren til USA for jobbintervju. Da han landet i USA ble han bedt om å bevise sine ferdigheter i å bryte seg inn i datanettverk. Det han ikke visste var at FBI benyttet seg av et dataprogram som tok opp hans brukernavn og passord til hans datamaskiner i Russland. Hackeren ble arrestert og ved bruk av hans passord og brukernavn, ble bevis for de straffbare forhold lastet ned fra hans russiske datamaskiner. Bevismaterialet ble senere benyttet for å dømme ham i straffesaken mot ham.

I tillegg til at det ved datakriminalitet i mange tilfeller kan være vanskelig å finne ut hvem som er gjerningspersonene, viser denne saken at det kan være vanskelig å få tak i vedkommende også når han er kjent. I ovennevnte sak ble FBI sitt angrep på hackerens datamaskiner i Russland oppfattet som et brudd på Russisk suverenitet.

Det enkelte lands utleveringslover kan sette skranker for muligheten til å strafforfølge utlendinger i Norge selv om den straffbare handlingen faller inn under norsk jurisdiksjon. Etter utleveringsloven § 2 kan for eksempel ikke norske statsborgere utleveres. Lov om utlevering av lovbrytere til Danmark, Finland, Island og Sverige (lov av 3. mars 1961 nr.1) gir en begrenset adgang til å utlevere norske statsborgere til disse landene.

Innenfor området for Schengenavtalen (konvensjon om gjennomføring av Schengenavtalen av 14. juni 1985), omfatter samarbeidet blant annet politisamarbeid og plikt til å yte gjensidig hjelp under etterforskning (kapittel 1 og 2). Avtalen har også regler om utlevering (kapittel 4).

Videre er det begrensninger i adgangen til å strafforfølge et forhold som er pådømt i utlandet. Dette følger av § 8 i den nye straffeloven alminnelige del. Her henvises det til de norske utleveringslovene samt til Schengenavtalen. Det vises her til forarbeidene til § 8 i blant annet Ot.prp. nr. 90 (2003-2004) kapittel 13.5.

## 8.8 Internasjonalt lovarbeid – veien videre

Utvalget understreker behovet for norsk deltakelse i videre internasjonalt lovsamarbeid når det gjelder datakriminalitet og strafforfølgning. Felles regelverk som sikrer både en kriminalisering av datakriminalitet og muligheten for å faktisk gjennomføre strafforfølgning er helt avgjørende dersom man skal klare å bekjempe trusselen som datakriminalitet representerer overfor det moderne samfunn.

På nettavisen digi.no kunne man den 5. oktober 2006 lese om en sak hvor tre russere ble dømt i Russland for datainnbrudd og for å ha presset britiske nettsteder for penger. Angrepene var rettet mot britiske nettkasinoer og bookmakere. De tre brukte et egenutviklet program for å samle opplysninger om nettstedene. Deretter advarte de nett-

stedene om at de ville stenge dem dersom de ikke betalte. Da et av de britiske selskapene nektet å betale, stengte de tre utpresserne selskapets nettsted under Breeder's cup-løpene med det til følge at selskapet ble påført et daglig tap på 200 000 dollar. Til sammen skal de tre ha presset over 4 millioner dollar fra britiske selskaper. De var aktive i seks måneder og angrep 54 selskaper fordelt på 30 land. I september 2004 ble de alle arrestert, da etter et samarbeid mellom russisk politi, det britiske politiets Serious Organized Crime Agency (SOCA), det amerikanske føderale politiet FBI samt Interpol. Håndteringen av denne saken viser de involverte lands erkjennelse av at denne type grenseløse økonomiske kriminalitet krever et omfattende internasjonalt politisamarbeid. Saken viser også hvordan slikt samarbeid kan lykkes.

Det viktigste synes altså å være å arbeide aktivt for mer internasjonal lovgivning som også setter standarder for internasjonalt samarbeid om strafforfølgning.

# Kapittel 9
# Spesielle motiver

## 9.1 Utkastet § 1. Definisjoner

Utkastet § 1 inneholder legaldefinisjoner av de mest sentrale begrepene i lovforslaget. I kapittel 5.2 er det redegjort for de generelle overveielsene knyttet til begrepsbruken.

### 9.1.1 Utkastet § 1 bokstav a. Datasystem

Utkastet § 1 bokstav a lyder:

> «Datasystem: Enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogram.»

«Datasystem» er benyttet i følgende bestemmelser i datakrimkapitlet: § 2 (elektronisk kartlegging), § 3 (ulovlig anbringelse av utstyr m.v.), § 4 (ulovlig tilgang til datasystem), § 8 (uberettiget bruk av datasystem m.v.), § 10 (ulovlig befatning med tilgangsdata), § 12 (selvspredende dataprogram), § 13 (driftshindring) og § 16 (kontomisbruk).

«Datasystem» er et infrastrukturbegrep på linje med «elektronisk kommunikasjonsnett», jf. utkastet § 1 bokstav e. Se kapittel 9.1.5 om dette.

Uttrykket «enhver innretning» favner vidt, men er knyttet til vilkårene om at innretningen må bestå av «maskinvare og data» og at den må kunne foreta «behandling av data ved hjelp av dataprogram».

«Maskinvare» er fysisk utstyr.

«Data» er benyttet to ganger i definisjonen og har likt betydningsinnhold. Begge steder skal begrepet forstås som den informasjon som er omfattet av datadefinisjonen i utkastet § 1 bokstav c første punktum. Dette er elektroniske signaler som kan lagres eller behandles av et datasystem (eller kan overføres i et elektronisk kommunikasjonsnett). Den informasjon som er «data», jf. utkastet § 1 bokstav c annet punktum, er ikke direkte relevant i forhold til definisjonen av «datasystem», siden den må omformes til elektroniske signaler for å kunne behandles i et datasystem. Slik omforming kan for eksempel skje ved bruk av en skanner. En microfichleser er «teknisk utstyr» som nevnt i bokstav c annet punktum, og oppfyller ikke i seg selv vilkårene for å være et «datasystem», jf. bokstav a, se mer om dette nedenfor.

I definisjonen av «datasystem» benyttes «data» som betegnelse både for programutrustning og styringsfiler som sørger for datasystemets funksjonalitet og sikkerhet (aktiv form), og for de data som er gjenstand for lagring eller behandling på datasystemet (passiv form). I uttrykket «maskinvare og data» skal data forstås i denne tosidige betydningen. I den del av definisjonen som gjelder «behandling av data» ved hjelp av dataprogram, har databegrepet passiv betydning, det vil si er gjenstand for automatisk behandling (herunder lagring).

For øvrig er «dataprogram» en underkategori av data, jf. utkastet § 1 bokstav b (se neste kapittel) og omfattes av databegrepet begge steder det er benyttet i utkastet § 1 bokstav a.

Av det foregående følger det at enhver innretning som kan foreta automatisk behandling av data er et «datasystem». Både av uttrykket «enhver innretning» og det at datadefinisjonen er sentral for innholdet i begrepet, følger det at «datasystem» skal forstås uavhengig av hvilket formål det tjener, hvilke tjenester det yter, hvilken samfunns- eller mediesektor det betjener og hvilket innhold det behandler. Eksempler på hva som omfattes er personlige datamaskiner, datamaskiner og servere som tilhører eller står i en bedrift, i den offentlige forvaltning, på internett, mobiltelefon, personlig digital assistent (PDA), rutere, basestasjoner, kringkastingssendere osv.

I kapittel 5.2.2 er det redegjort for at flere datasystemer kan inngå i et nett og som helhet anses som ett større datasystem. Det er også redegjort for at datasystem kan være komponent i et elektronisk kommunikasjonsnett, jf. utkastet § 1 bokstav e, og omfattes av formuleringen «annet koplings- eller dirigeringsutstyr». Likeledes kan et elektronisk kommunikasjonsnett være komponent i et datasystem.

Vilkåret om at innretningen må kunne foreta behandling av data ved hjelp av dataprogram innebærer en avgrensning overfor komponenter og periferienheter som ikke oppfyller dette vilkåret selvstendig sett. En harddisk eller minnepinne som er koblet til en prosessor, er del av et «datasystem», men dersom den er koblet fra og for eksem-

pel ligger løst i en hylle, er den å anse som et lagringsmedium som ikke alene er et «datasystem». Definisjonen inneholder ikke noen formulering som åpner for at *del av* et datasystem er omfattet selvstendig sett. Det er vanlig at en innretning som utfører automatisk databehandling består av forskjellige komponenter som kan kobles til og fra. Det er altså bare når komponentene er sammenkoblet at de utgjør den innretning som anses som datasystem. Av dette følger også at en innretning oppfyller vilkårene for å være datasystem når det er bygd opp av ulike komponenter som til sammen evner å utføre automatisk databehandling.

Andre eksempler på slike komponenter eller periferienheter er tastatur, mus, cd, dvd og harddisk.

### 9.1.2 Utkastet § 1 bokstav b. Dataprogram

Utkastet § 1 bokstav b lyder:

> «Dataprogram: Data i form av en sekvens instruksjoner som kan utføres i et datasystem, herunder kildekode.»

«Dataprogram» er benyttet i følgende bestemmelser i datakrimkapitlet: § 3 annet ledd (ulovlig anbringelse av utstyr m.v.), § 11 (skadelig dataprogram og utstyr) og § 12 (selvspredende dataprogram). Ifølge gjerningsbeskrivelsen i disse bestemmelsene er dataprogram et verktøy for å begå den ulovlige handling. Men selve definisjonen som sådan er deskriptiv og verken positivt eller negativet ladet.

«Dataprogram» er en underkategori av «data» og befinner seg som sådan på nivå over infrastrukturbegrepene. Se kapittel 5.2.2 om dette.

Definisjonen omfatter alle utviklingsstadier av et dataprogram, fra det skrives i kildekode, til det er kompilert og kan anvendes av en datamaskin (objektkode). Vilkåret er at det foreligger elektronisk, jf. betingelsen om at det må være «data», jf. definisjonen i utkastet § 1 bokstav c. Data er informasjon som er lesbar for en datamaskin. Kildekode som er skrevet på papir faller derfor utenfor definisjonen av dataprogram.

Sentralt i definisjonen er «sekvens instruksjoner som kan utføres i et datasystem». Informasjonen må altså gå ut på å instruere et datasystem, det vil si styre dets funksjoner eller prosesser, men som nevnt er det ikke noe vilkår at programmet er kompilert slik at det uten videre kan anvendes av datamaskinen.

Det vises ellers til bemerkningene om data i neste kapittel.

### 9.1.3 Utkastet § 1 bokstav c. Data

Utkastet § 1 bokstav c lyder:

> «Data: Enhver representasjon av informasjon som lagres eller behandles av et datasystem eller som overføres i et elektronisk kommunikasjonsnett. I tillegg omfattes enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk utstyr.»

«Data» er benyttet i følgende bestemmelser i datakrimkapitlet, og da som betegnelse på det vernede objekt etter bestemmelsen: § 6 (datatyveri), § 7 (datamodifikasjon), § 9 (etterfølgende befatning med data og databasert informasjon m.v.) og § 10 (ulovlig befatning med tilgangsdata). I tillegg benyttes «data» i § 13 (driftshindring), men her for å betegne verktøyet for overtredelsen.

«Data» er signaler som lagres, behandles eller overføres over en infrastruktur og er følgelig på nivået over infrastrukturen i begrepshierarkiet. Det samme gjelder «dataprogram». Se kapittel 5.2.2 om dette.

«Data» er nøkkelbegrepet som de andre definisjonene bygger på, dog slik at definisjonen av «elektronisk kommunikasjonsnett» anvender formuleringen «elektronisk kommunikasjon» i stedet for «data som overføres», for å oppnå identitet med definisjonen i ekomloven.

Datadefinisjonen består av to punkter. Den viktigste fellesnevneren er at dataene krever teknisk utstyr for å kunne utnyttes. Det tekniske utstyret kan være «datasystem» eller «elektronisk kommunikasjonsnett», jf. første punktum, eller utstyr av annen art, jf. annet punktum, for eksempel en hullkortmaskin eller microfichleser. Etter definisjonen er «data» med andre ord ikke lesbar eller forståelig for et menneske, men for en maskin. Definisjonens annet punktum benytter ordet «lesbar», og av sammenhengen fremgår det at dette ikke innebærer at informasjonen skal være direkte lesbar for et menneske. Her betyr ordet «lesbar» at informasjonen lar seg registrere av dertil egnet teknisk utstyr, jf. eksemplene nevnt ovenfor. Når dataene foreligger i en slik representasjon at de er forståelige for et menneske, anses de som «databasert informasjon», jf. utkastet § 1 bokstav d.

Både første og annet punktum i datadefinisjonen benytter uttrykket «enhver representasjon av informasjon». Meningen er å få frem at hvilket innhold informasjonen har er uten betydning for om det er «data». Datadefinisjonen er utelukkende basert på tekniske kriterier. Dette er i samsvar med datakrimkonvensjonens krav, jf. definisjonen av «computer data» i artikkel 1, se merknadene i kapittel 5.2.1. Vilkårene etter første punktum er at informasjonen er

representert i en slik form at den kan lagres eller behandles av et datasystem, eller overføres i et elektronisk kommunikasjonsnett. Første punktum gjelder følgelig elektroniske signaler, siden det bare er slike som kan utnyttes i datainfrastrukturen. Om forståelsen av begrepene «datasystem» og «elektronisk kommunikasjonsnett» vises det til de generelle merknadene i kapittel 5.2.2 og i særmerknadene i kapittel 9.1.1 og 9.1.5.

Annet punktum gjelder informasjon som ikke kan utnyttes av et datasystem eller i et elektronisk kommunikasjonsnett direkte, men som foreligger i en form som forutsetter bruk av teknisk utstyr for å kunne utnyttes, jf. de tidligere kommentarer om dette. Det kan for eksempel være tale om informasjon lagret på hullkort, på glassplate (microfich) og i integrerte kretser.

Det sentrale vilkår er at informasjonen «ikke er lesbar uten bruk av teknisk utstyr». Den vil altså ikke kunne gi mening for et menneske uten teknisk konvertering. Avgrensningen mot første punktum innebærer at den heller ikke kan anvendes direkte i datainfrastrukturen som nevnt, uten slik konvertering.

Annet punktum i definisjonen av data sørger for at maskinlesbar informasjon som ikke er elektroniske signaler, får et rettslig vern mot datakriminalitet. Dette er i samsvar med gjeldende rett, i hvert fall for så vidt gjelder uberettiget adgang til data, jf. straffeloven § 145 annet ledd. Det vises til bemerkningene i kapittel 5.2.2 om dette. De mest praktiske overtredelsesformer av straffebudene i utkastet §§ 6, 7, 9 og 10 hvor databegrepet er benyttet, vil nok være rettet mot data som definert i utkastet § 1 bokstav c første punktum. Men det er for eksempel tenkelig med tyveri av data som nevnt i bokstav c annet punktum, dersom det foretas uberettiget eksemplarfremstilling av en microfich eller av et hullkort. Videre kan man tenke seg datamodifikasjon begått ved å stanse ut uriktige hull i eldre hullkort. Det vises ellers til merknadene til de respektive straffebudene.

Siden innholdet er uten betydning for om en representasjon av informasjon er data, kan det slås fast at data kan inneholde enhver tenkelig type informasjon som tekst, lyd, bilde og dataprogram. Det er uten betydning om innholdet har økonomisk verdi og hvilke interesser eller rettigheter som måtte være knyttet til innholdet. Se merknadene i kapittel 5.2. Sett i forhold til gjeldende bestemmelser dekker databegrepet følgelig «data og programutrustning» i straffeloven §§ 145 annet ledd og 270 første ledd nr. 2, «telefonsamtale» og «opptak» i straffeloven § 145 a, «tilgangsdata» i straffeloven § 145b, «vernede tjenester» i straffeloven § 262 fjerde ledd og digitaliserte vernede verk i åndsverkloven § 1, som har et straffesanksjonert vern mot uberettiget beskyttelsesbrudd, kopiering og tilgjengeliggjøring for allmennheten, jf. § 2, jf. § 53a, jf. § 54 første ledd bokstav b. Denne opprams-singen av bestemmelser er ikke uttømmende, men angir noen praktiske områder for databegrepet, jf. definisjonen i lovforslaget.

Datadefinisjonen i bokstav c første punktum omfatter uttrykkelig data som kan lagres, behandles eller overføres. Om bakgrunnen for å ta med alternativet «behandles» vises det til merknadene i kapittel 5.2.2 i underkapitlet «Data og dataprogram». Ved fortolkningen av de straffebud som benytter ordet «data», må det tas hensyn til at definisjonen omfatter data i ulike tilstander. For eksempel datatyveribestemmelsen i utkastet § 6 rammer dermed kopiering av data som er lagret, og kopiering og tapping av en datastrøm, for eksempel på et datanettverk.

### 9.1.4 Utkastet § 1 bokstav d. Databasert informasjon

Utkastet § 1 bokstav d lyder:

> «Databasert informasjon: Meningsinnholdet i data. »

«Databasert informasjon» er benyttet i følgende bestemmelser i datakrimkapitlet: § 5 (informasjonstyveri), § 9 (etterfølgende befatning med data og databasert informasjon m.v.) og § 10 (ulovlig befatning med tilgangsdata).

«Databasert informasjon» er på øverste nivå i begrepshierarkiet, og det er på dette nivået – eller stadiet i formidlingsprosessen – at et menneske kan gjøre seg kjent med innholdet. Det vises til kapittel 5.2.2 om dette. Vilkåret om at meningsinnholdet må være knyttet til «data» innebærer en viktig avgrensning mot meningsinnhold som formidles av andre informasjonsbærere (medier). Skrift på papir er ikke meningsinnholdet i «data». Dette gjelder selv om det er tale om en utskrift fra en datamaskin. Derimot omfattes innhold som kan leses på en skjerm, eller som kan høres, det vil si audiovisuelle sanseopplevelser formidlet fra data.

Vilkåret om at informasjonen skal kunne gi mening for et menneske ligger i uttrykket «meningsinnholdet». Dette gir anvisning på at det må kunne skje en menneskelig tolkning av informasjonen, men innebærer ikke noe vilkår om at informasjonen er forståelig eller faktisk ble forstått i et konkret tilfelle. Det er tilstrekkelig at den kan oppfattes (høres, ses, eller eventuelt føles, dersom det for eksempel gjelder dataimpulser som formidles til blinde). Det vesentlige er at det avgrenses

mot informasjon som bare kan «leses» av en datamaskin eller annet teknisk utstyr, som er «data», jf. utkastet § 1 bokstav c. Et dataprogram i objektkode som bare kan leses av en datamaskin er ikke meningsinnholdet i data. Men kildekoden kan være databasert informasjon, for eksempel dersom den fremvises på dataskjermen slik at et menneske kan lese den.

Eksempler på «databasert informasjon» er innholdet (lyd og bilde) som formidles på skjermen til et fjernsynsapparat, en datamaskin eller en mobiltelefon, eller rent auditivt via lydbånd, cd- og mp3-spiller, i telefonsamtale osv.

Data kan være lagret, under behandling eller overføring, jf. definisjonen i bokstav c. Det samme gjelder følgelig meningsinnholdet i data, jf. bokstav d. Dette har særlig betydning i utkastet § 5 om informasjonstyveri, som dermed for eksempel omfatter både at et menneske uberettiget leser databasert informasjon fra en skjerm, og at et menneske avlytter en telefonsamtale mens den pågår (meningsinnholdet i data under overføring).

### 9.1.5 Utkastet § 1 bokstav e. Elektronisk kommunikasjonsnett

Utkastet § 1 bokstav d lyder:

> «Elektronisk kommunikasjonsnett: System for elektronisk kommunikasjon der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår.»

«Elektronisk kommunikasjonsnett» er benyttet i følgende bestemmelser i datakrimkapitlet: § 2 (elektronisk kartlegging), § 3 (ulovlig anbringelse av utstyr m.v.), § 8 (ulovlig bruk av datasystem m.v.), og § 13 (driftshindring). I §§ 2 og 3 anvendes begrepet for å beskrive den straffbare fremgangsmåten. I de øvrige bestemmelsene angir begrepet det vernede objekt.

Definisjonen er likelydende med ekomlovens definisjon, jf. ekomloven § 1-5 nr. 2, se også bemerkningene i kapittel 5.2.3. Hensynet til begrepsharmonisering med ekomloven har medført at definisjonen inneholder uttrykket «elektronisk kommunikasjon» i stedet for «data som overføres», jf. formuleringen i datadefinisjonen i utkastet § 1 bokstav c. Uttrykkene er imidlertid ment å bety det samme.

I kapittel 5.2.3 er det redegjort for at elektronisk kommunikasjonsnett kan være del av et datasystem og vice versa. Når datasystem inngår i elektronisk kommunikasjonsnett omfattes det av formuleringen «annet koplings- og dirigeringsutstyr», jf. utkastet § 1 bokstav d.

## 9.2 Utkastet § 2. Elektronisk kartlegging

Utkastet § 2 lyder:

> «For elektronisk kartlegging av datasystem straffes den som over et elektronisk kommunikasjonsnett uberettiget registrerer egenskaper på et datasystem for å kartlegge sårbarheter.
>
> Straffen er bøter eller fengsel inntil 6 måneder. For grov overtredelse er straffen bøter eller fengsel inntil 1 år.»

Det vises til merknadene i kapittel 5.4.2.

Straffebudet rammer kartleggingsvirksomhet rettet mot andres datasystem. Straffebudet presiserer ikke uttrykkelig at datasystemet må tilhøre en annen, men vilkåret følger implisitt av at kartlegging av egenskaper på eget system ikke kan tenkes å være en rettsstridig handling.

Kartleggingsvirksomheten må skje via det elektroniske kommunikasjonsnettet, jf. formuleringen «over et elektronisk kommunikasjonsnett». Dette avgrenser straffebudet overfor kartlegging som skjer ved fysisk observasjon av et datasystem, eventuelt ved at det fotograferes eller lignende.

Den kartleggingsvirksomhet som rammes, skjer altså ved hjelp av dertil egnet programvare som utnyttes over det elektroniske kommunikasjonsnettet. Det er et vilkår at kartleggingen har som formål å avdekke sårbarheter på det datasystem som utsettes for kartleggingen. Med «sårbarheter» menes områder på datasystemet som lar seg misbruke for å skaffe ulovlig tilgang til datasystem, jf. utkastet § 4. Denne kunnskap om sårbarheter oppstår som følge av at kartleggingen avdekker at datasystemet er satt opp med programvare eller tjenester med kjente sikkerhetshull. De opplysninger som avdekkes av kartleggingsvirksomheten må altså kombineres med gjerningspersonens egen kunnskap om datasystemers sårbarheter. Slik kunnskap kan gjerningspersonen skaffe seg ved å benytte et kartleggingsverktøy som er programmert for å identifisere slike sårbarheter og varsle ham om det. Deretter er systemet sårbart for inntrengning, jf. utkastet § 4, datamodifikasjon, jf. utkastet § 7, og uberettiget bruk, jf. utkastet § 8.

## 9.3 Utkastet § 3. Ulovlig anbringelse av utstyr m.v.

Utkastet § 3 lyder:

> «For ulovlig anbringelse av utstyr straffes den som uberettiget anbringer utstyr på eller i til-

knytning til et datasystem eller elektronisk kommunikasjonsnett, for å

a) begå informasjons- eller datatyveri, jf. §§ 5 og 6, eller
b) tilegne seg tilgangsdata som nevnt i § 10.

Det samme gjelder den som installerer dataprogram på et datasystem for å begå handlinger som nevnt.

Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen fengsel inntil 3 år.»

Det vises til merknadene i kapittel 5.4.3.

Straffebudet rammer anbringelse av «utstyr» (første ledd) eller installering av «dataprogram» (annet ledd) for å tilegne seg informasjon slik som beskrevet i første ledd bokstav a og b.

«Utstyr» i første ledd betyr fysisk utstyr som anbringes på eller i tilknytning til et datasystem eller elektronisk kommunikasjonsnett. Det kreves ikke at utstyret i seg selv kan karakteriseres som ulovlig. Det er bruken, det vil si anbringelsen av utstyret for å oppnå et formål som angitt i bokstav a eller b, som er straffbar. Eksempel på hva som omfattes av første ledd er et videokamera som monteres i nærheten av en minibank for å filme tastetrykk, en «falsk front» eller mekanisk tastetrykksregistrator som monteres på selve minibanken, avlyttingsutstyr som monteres i en telefonsentral (datasystem) eller på det elektroniske kommunikasjonsnettet, og en fysisk tastetrykksregistrator som monteres på tastaturkabelen til et datasystem.

Av formuleringen «på eller i tilknytning til» følger det at det ikke er noen betingelse at utstyret anbringes direkte på det datasystem eller elektroniske kommunikasjonsnett som kan avgi informasjon som nevnt i bokstav a og b. Ofte er det aktuelt å plassere utstyret «på» objektet, som for eksempel den falske fronten eller avlyttingsutstyret, mens et videokamera vil kunne anses plassert «i tilknytning til» objektet. Det er tilstrekkelig for oppfyllelse av tilknytningskriteriet at utstyret er slik plassert at det kan fange opp informasjonen som nevnt.

Etter annet ledd er det straffbart å installere «dataprogram på et datasystem». Dette alternativet dekker det samme tilfellet som nevnt i første ledd når fremgangsmåten baserer seg på bruk av et dataprogram. Et praktisk eksempel er installering av en nettverkssniffer for å avlytte data som overføres på det elektroniske kommunikasjonsnettet. Snifferen er installert på datasystemet som står i nettet, og registrerer den trafikk som passerer, også trafikk som ikke er adressert til en selv og som man følgelig er uberettiget til å registrere. Programmet kan også være satt opp til å fange opp passord som sendes over nettet, og fungerer da som en programvarebasert tastetrykksregistrator, se kapittel 3.4.6.

Hvorvidt datasystemet som dataprogrammet er installert på tilhører en selv eller en annen, er uten betydning for straffbarheten. Det vises til begrunnelsen i de generelle merknadene kapittel 5.4.3. Dersom installering skjer på en annens system vil det være aktuelt å anvende utkastet § 3 i idealkonkurrens med utkastet § 7 (datamodifikasjon).

Straffbar anbringelse eller installering etter første og annet ledd er betinget av at det skjer for å utføre handlinger som beskrevet i første ledd bokstav a eller b.

Alternativet i første ledd bokstav a rammer det «å begå informasjons- eller datatyveri, jf. §§ 5 og 6». Det vises til merknadene til disse bestemmelsene. Eksempelvis vil plassering av avlyttingsutstyr kunne straffes etter utkastet § 3 første ledd bokstav a, jf. utk § 5, dersom det skal lyttes samtidig som utstyret er i bruk, eller, jf. utkastet § 6, dersom avlyttingsutstyret direkte benyttes for tapping av data under overføring som lagres til et lagringsmedium.

Alternativet i første ledd bokstav b gjelder det «å tilegne seg tilgangsdata som nevnt i § 10». Mens utkastet § 10 rammer den konkrete rettsstridige befatning med tilgangskodene, herunder anskaffelse og fremstilling, rammer utkastet § 3 første ledd bokstav b, plassering av utstyr eller dataprogram for å anskaffe eller fremstille tilgangskodene. Anbringelse av et videokamera ved en minibank for å fange opp tastetrykk, og av dataprogram for å registrere passord som sendes over nettet, er praktiske eksempler på hva som omfattes av dette alternativet.

Subjektivt kreves det forsett. Dette gjelder også for alternativene i bokstav a og b, jf. formuleringen «for å». Det er tilstrekkelig å bevise at gjerningspersonen på tidspunktet for anbringelse eller installering, var klar over at utstyret eller dataprogrammet ville skaffe informasjon som nevnt i bokstav a og b, når det ble tatt i bruk eller aktivisert.

## 9.4 Utkastet § 4. Ulovlig tilgang til datasystem

Utkastet § 4 lyder:

«For ulovlig tilgang straffes den som uberettiget skaffer seg tilgang til hele eller del av et datasystem.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.»

Det vises til de uførlige merknadene i kapittel 5.6.2.

Nøkkelformuleringen er «hele eller del av et datasystem». Datasystem er definert i utkastet § 1 bokstav a, og er koblet til begrepet «data», jf. utkastet § 1 bokstav c. Av dette følger at det ikke har noen betydning hva slags datasystem det er tale om, dets formål, innehaverens virksomhet eller det innhold det behandler.

Bestemmelsen anvender ikke noe vilkår om beskyttelsesbrudd, se begrunnelsen i kapittel 5.6.2. I praksis vil imidlertid beskyttelsesbrudd (som passordinnbrudd) og fremgangsmåter som har vært likestilt med dette (som sårbarhetsinnbrudd) være en praktisk overtredelsesmåte. Disse fremgangsmåtene er beskrevet i kapittel 3.4.1. Dersom tilgangen skjer ved beskyttelsesbrudd skal det tas i betraktning som en skjerpende omstendighet ved handlingen, jf. utkastet § 18.

Bestemmelsen rammer selve den uberettigete tilgang. En naturlig følge av slik tilgang vil være at data på systemet ulovlig tilegnes, eventuelt at datasystemet tas i ulovlig bruk. Dette er handlinger som i tid kommer etter at tilgang er oppnådd og som straffes av andre bestemmelser i lovforslaget, jf. utkastet §§ 5, 6 og 8. Disse bestemmelsene kan derfor anvendes i realkonkurrens med utkastet § 4. Vilkåret om tilgang innebærer en avgrensning mot elektronisk kartlegging av datasystem. Slik kartlegging gir ikke «tilgang» til datasystemet eller noen del av dette. Kartlegging rammes som en selvstendig straffbar handling, jf. utkastet § 2.

## 9.5 Utkastet § 5. Informasjonstyveri

Utkastet § 5 lyder:

> «For informasjonstyveri straffes den som uberettiget tilegner seg
> a) databasert informasjon, eller
> b) utskrift av databasert informasjon.
>
> Straff etter første ledd bokstav b kommer ikke til anvendelse ved handling som går inn under § 257 (tyveribestemmelsen).
>
> Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.»

Det vises til de generelle merknadene i kapittel 5.5.1 og 5.5.2.

Straffebudet gjelder uberettiget tilegnelse av databasert informasjon (første ledd bokstav a) og av utskrift av databasert informasjon (første ledd bokstav b). Bestemmelsen gir et generelt vern mot informasjonstyveri uavhengig av karakteren av innholdet. Supplementet i første ledd bokstav b er nødvendig for å fange opp handlinger som har nær sammenheng med tilegnelse av databasert informasjon. Tilegnelse av databasert informasjon, jf. første ledd bokstav a, innebærer et vilkår om at handlingen skjer direkte overfor det databaserte innholdet, for eksempel ved avlesing av et skjermbilde eller avspilling av et båndopptak. Papirutskrifter omfattes ikke av dette alternativet. Uten supplementet i første ledd bokstav b vil ikke slike papirutskrifter ha noe tilfredsstillende strafferettslig vern mot uberettiget tilegnelse. Det vises til merknadene i kapittel 5.5.2 om dette.

Straffebudet er på samme vis som de øvrige bestemmelser i lovforslaget, innholds- og teknologinøytralt. Det dekker følgelig databasert informasjon av enhver karakter. Vilkåret er at tilegnelsen er rettsstridig. I den grad tilegnelsen gjelder opphavsrettslig vernet materiale må rettsstridsreservasjonen som i dag står i åndsverkloven § 53a tredje ledd annet punktum, iakttas.

Informasjonstilegnelsen kan gjelde data som er lagret, behandles eller som overføres. Dette følger av koblingen mellom definisjonen av «databasert informasjon» i utkastet § 1 bokstav d, jf. definisjonen av «data» i utkastet § 1 bokstav c. Eksempler på databasert informasjon under overføring kan være telefonsamtaler, internettkommunikasjon og datakommunikasjon på et bedriftsnett. Videre kan det omfatte overføring av radio- og kringkastingssignaler og av informasjonssamfunnstjenester, jf. gjeldende bestemmelse i straffeloven § 262 fjerde ledd. Tilegnelseshandlingen vil bestå i å se eller lytte til kommunikasjonsstrømmen, fordi sansebruken er en betingelse for at den kan anses som «meningsinnhold i data». Det samme gjelder overføringen av beskyttede vernede verk, jf. åndsverkloven § 53a første ledd, jf. § 2 siste ledd. En tilegnelse som utelukkende består i å kopiere eller tappe kommunikasjonsstrømmen uten å se eller lytte til denne, er eventuelt et datatyveri som kan rammes av utkastet § 6.

## 9.6 Utkastet § 6. Datatyveri

Utkastet § 6 lyder:

> «For datatyveri straffes den som uberettiget kopierer, overfører eller på annen måte tilegner seg data.
>
> Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder. »

Det vises til de generelle merknadene i kapittel 5.5.1 og 5.5.2.

Straffebudet er på samme vis som de øvrige bestemmelser i lovforslaget, innholds-, teknologi- og medienøytralt. Data er representasjon av informasjon som kan lagres eller behandles av et datasystem eller overføres i et elektronisk kommunikasjonsnett. I tillegg omfattes annen representasjon av informasjon som krever bruk av teknisk utstyr for å være lesbar, se utkastet § 1 bokstav c. Straffebudet rammer følgelig handlinger hvor tilegnelsen skjer maskinelt. Tilegnelse ved sansebruk rammes av utkastet § 5.

Tilegnelsen kan bestå i å kopiere eller overføre data. I tillegg omfattes andre varianter gjennom sekkealternativet «på annen måte». Dette alternativet er antakelig mest aktuelt når det er tale om å tilegne seg data som nevnt i utkastet § 1 bokstav c annet punktum. Se kapittel 9.1.3 om dette.

Kopiering innebærer å lage et duplikat av dataene. For at det skal anses som en «tilegnelse» må kopien flyttes til et sted utenfor den berettigedes kontroll, for eksempel ved at data kopieres fra en bedriftsserver til cd-rom som lovovertrederen disponerer. Det er ikke noe vilkår at cd-platene faktisk er ført ut av bedriften. Det er tilstrekkelig for fullbyrdet tilegnelse at dataene er overført til cd-platene, når dette må anses som rettsstridig i forhold til den berettigete. Rettsstriden må avgjøres på grunnlag av en totalvurdering av situasjonen og de aktuelle regler og retningslinjer som kan være relevant i en slik situasjon. Se merknadene i kapittel 5.3. Data lar seg imidlertid også kopiere innenfor samme datasystem. Dersom man på denne måte dupliserer eller eventuelt flytter rundt på data på et system, vil de normalt fremdeles være under den berettigetes rådighet. Forutsatt at kravet til rettsstrid er oppfylt er det mest nærliggende å bedømme et slikt tilfelle etter reglene om datamodifikasjon og uberettiget bruk av datasystem, jf. utkastet §§ 7 og 8. Det stilles spørsmål om dataene i dette tilfellet kan anses å være tilegnet slik at forholdet skal subsumeres som datatyveri. Problemstillingen kan sammenlignes med nedre grense for tyveri, se Rt. 1894 side 484.

Alternativet «overfører» tar sikte på at data utføres fra det sted de ordinært behandles eller lagres, ved bruk av en elektronisk kommunikasjonstjeneste. For eksempel kan data tilhørende en bedrift kopieres og overføres til lovovertrederen selv, som vedlegg til en e-post som går til hans private konto.

I alle de nevnte tilfelle taper den berettigete kontrollen med spredningen av dataene, og dette er avgjørende for om det foreligger en fullbyrdet tilegnelse. Det er som nevnt tilstrekkelig at kopieringen eller overføringen skjer til andre lagringsmedier eller kommunikasjonstjenester enn de som ordinært skal anvendes til oppbevaring av dataene. Spesielt med tanke på frittstående lagringsmedier, er det ikke noe vilkår for fullbyrdelse at lagringsmediene med de kopierte dataene rent faktisk er tatt ut av det fysiske området som den berettigete kontrollerer. Dette kan være særlig relevant med tanke på datatyveri i arbeidsforhold.

Tilegnelse kan også skje overfor data som overføres. Kopieringen, som også kalles tapping, skjer da mens kommunikasjonen pågår. Såfremt det bare er tale om kopiering til en lagringsenhet, som til en båndopptaker eller en datamaskin som lagrer større mengder data, eventuelt til cd-er m.v., er handlingen et datatyveri. Dersom lovovertrederen lytter til – eventuelt ser på – signalene samtidig som de kopieres, foreligger i tillegg et informasjonstyveri, jf. § 5. Dette utløser et konkurrensspørsmål mellom utkastet §§ 5 og 6 som må løses etter en totalvurdering av den konkrete situasjon.

## 9.7 Utkastet § 7. Datamodifikasjon

Utkastet § 7 lyder:

> «For datamodifikasjon straffes den som uberettiget endrer, ødelegger, sletter eller skjuler andres data.
>
> Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen bøter eller fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.»

Det vises til merknadene i kapittel 5.6.3.

Dette straffebudet gir data et selvstendig vern mot skadevoldende handlinger. Data er definert i utkastet § 1 bokstav c. Skadevoldende handlinger rettet mot det fysiske utstyret (datainfrastrukturen) skal bedømmes etter andre straffebud om fysisk skadeverk.

Straffebudet oppstiller flere likestilte alternative overtredelsesformer, jf. «endrer, ødelegger, sletter eller skjuler andres data». Disse alternativene beskriver integritetskrenkelser overfor data og betegnelsen på handlingene er følgelig «datamodifikasjon» (se merknader om denne terminologien i kapittel 4.6.2). Objektet for integritetskrenkelsen kan være en enkelt datafil, som for eksempel rettsstridig sletting av en annens word-dokument. Men selv om handlingen rent isolert sett rammer en enkelt fil kan den utgjøre en integritetskrenkelse overfor datasystemet som sådan. Dette kan være tilfelle dersom slettingen gjelder en vik-

tig programfil som styrer prosessene på systemet. Følgen av handlingen er at datasystemet er ute av stand til å utføre de prosesser som ville fulgt av programmet.

Straffebudet stiller imidlertid ikke noe krav til følgen av handlingen, men følgen kan få betydning for om handlingen er grov eller liten, jf. utkastet §§ 18 og 19 og for straffutmålingen.

De ovennevnte eksempler gjelder handlinger voldt overfor data organisert i filsystemer, men det er ikke noe vilkår at objektet er en data*fil*. Enhver krenkelse som nevnt overfor data er omfattet av straffebudet, for eksempel integritetskrenkelser overfor data organisert i en database. Som et eksempel fra rettspraksis kan det vises til Rt. 2004 side 94, hvor domfelte slettet alle data i en kundedatabase.

Alternativet «endrer» er hovedalternativet. I realiteten dekkes de øvrige alternativene langt på vei av «endrer». Når de likevel er inntatt i straffebudet skyldes det pedagogiske og informative grunner. Det blir lettere i praksis å se hvordan bestemmelsen kommer til anvendelse.

Alternativet «endrer» må også avgrenses mot handlinger som rammes av utkastet § 8 om ulovlig bruk av datasystem. Den som benytter en annens datasystem for å skade innholdet gjør seg skyldig i overtredelse både av utkastet §§ 7 og 8. Men enhver bruk av datasystem innebærer at det skrives til systemet, og en slik tilførsel av data innebærer en endring etter ordlyden i utkastet § 7. Likevel skal ikke alle disse tilfellene anses som datamodifikasjon, jf. utkastet § 7, selv om *bruken* måtte være rettsstridig. Avgjørende er om endringen er rettet mot «andres data». Dette er forskjellig fra «andres datasystem», jf. utkastet § 8. Dersom en annens datasystem for eksempel tas i bruk for å lagre eget materiale (film, musikk, pornografi) er handlingen rettet mot datasystemets kapasitet (lagringsplass) og ikke mot data som ligger der fra før. Slik bruk vil kunne registreres i loggen og for så vidt innebære en endring i denne, men dette er heller ikke en endring etter utkastet § 7. Endringen i loggen er i et slikt tilfelle resultat av en ordinær funksjon på datasystemet. Dette skal altså eventuelt bedømmes etter utkastet § 8, forutsatt at bruken er rettsstridig.

Endring i utkastet § 7 innebærer at det foretas rettsstridige tilføyelser eller slettinger i eksisterende data slik at innholdet ikke lenger er slik som bestemt av den berettigete. Videre omfattes tilføyelser eller slettinger i programoppsettet ved tilførsel eller sletting av programfiler. Endringen i selve filen gjør at innholdet ikke lenger er intakt og dette er avgjørende, jf. utkastet § 7. Hvorvidt innholdet er blitt riktig eller galt (selv om det siste ofte vil være tilfelle) er uten betydning for straffbarheten. Den innholdsmessige siden gjelder kvalitetskriteriet, det vil si en egenskap som ikke omfattes direkte av integritetsvernet. Men integritet er en forutsetning for å kunne stole på at innholdet – og følgelig kvaliteten – er intakt. Det er altså en sammenheng mellom egenskapene.

Eksempler på endringer i data, jf. utkastet § 7, er å tilføye eller slette brukere i passordfilen, å slette innholdet i logger (for eksempel for å redusere muligheten for å bli oppsporet og strafforfulgt), å endre innholdet i en kildekode, og å endre innholdet i et word-dokument eller excel-fil.

Et eksempel på endringer i programoppsettet kan være å tilføye en «bakdør», det vil si åpne en tjeneste som skulle vært stengt slik at man lettere kan skaffe seg tilgang til systemet senere. Man kan også erstatte en programfil med en annen som inneholder avvikende egenskaper. En slik «utskifting» består i realiteten av flere handlinger (kommandoer), hvor det opprinnelige programmet slettes eller på annen måte settes ut av funksjon, og en tilførsel (kopiering) av det nye programmet. Tilfellet rammes således både av alternativet «endrer» og «sletter».

«Ødelegger» har liten selvstendig betydning ved siden av «endrer». Men dersom gjerningspersonen krypterer andres data, slik at de ikke lenger lar seg utnytte av den berettigete, er dette et treffende alternativ.

«Slette» betyr å fjerne data. Et praktisk eksempel er å slette logger for å fjerne spor etter egen straffbar handling. Formålet kan også være å svekke muligheten for å overvåke sikkerheten på datasystemet mer generelt.

Det kreves ikke at slettingen er utført så grundig at dataene ikke lar seg gjenskape. Enhver form for sletting omfattes. Også dette er en handling som grunnleggende sett er en variant av å endre data.

«Skjuler» kan gå ut på å kryptere andres data (som også kan anses som å ødelegge data), eller flytte data fra ett sted til et annet på datasystemet slik at de mister sin funksjon. Et eksempel kan være å flytte en html-fil inneholdende en hjemmeside på internett, slik at innholdet ikke lenger vises på internett. Filen kan likevel ligge intakt på datasystemet, bare slik at innholdet er blitt utilgjengeliggjort for omverdenen. Da er den «skjult», jf. utkastet § 7. Dersom filen flyttes helt vekk fra datasystemet, til et annet datasystem eller datalagringsmedium, anses handlingen som å slette data. I tillegg er det et datatyveri, jf. utkastet § 6.

Som det har fremgått kreves det ikke at skaden er uopprettelig. Iblant vil det være mulig å gjenskape slettede data ved å rekonstruere dem. Det kan også være at de data som har blitt utsatt for krenkelse finnes i form av en sikkerhetskopi som fremdeles er intakt. Like fullt foreligger en fullbyrdet overtredelse av utkastet § 7. Det er i samsvar med gjeldende rett, jf. straffeloven § 291, som også rammer skadeverk av midlertidig karakter. Se Rt. 1966 side 905 og Rt. 1986 side 571.

Rettslig sett kommer utkastet § 7 til anvendelse også på data som er lagret på andre tekniske lagringsmedier, jf. utkastet § 1 bokstav c annet punktum, for eksempel på hullkort, men det antas at slike overtredelser ikke er særlig praktiske. Det vises dog til eksemplet i kapittel 5.6.3.

Rt. 2004 side 1619 (videre kjæremål over lovanvendelsen) omhandler datamodifikasjon utført ved å foreta endring i passordliste og tilføyelse av «bakdør». Endringene hadde ikke betydning for brukerfunksjonaliteten, men hadde sikkerhetsmessige konsekvenser for systemet. Dette ble av Høyesterett bedømt som skadeverk, jf. straffeloven § 291. Utkastet § 7 viderefører denne rettstilstanden, dog slik at det ikke er nødvendig å vurdere konsekvensene for datasystemet. Det er tilstrekkelig å konstatere at integriteten av dataene er blitt krenket. Konsekvensene kan ha betydning for om lovbruddet anses grovt eller lite, jf. utkastet §§ 18 og 19.

## 9.8 Utkastet § 8. Uberettiget bruk av datasystem

Utkastet § 8 lyder:

> «For uberettiget bruk straffes den som uberettiget benytter andres datasystem eller elektroniske kommunikasjonsnett. Bruk av andres tilgangspunkt til internett i usikret trådløst elektronisk kommunikasjonsnett anses ikke som uberettiget.
>
> Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.»

Det vises til merknadene i kapittel 5.6.5.

Straffebudet rammer den som uberettiget benytter andres datasystem eller elektroniske kommunikasjonsnett, det vil si datainfrastrukturen som definert i utkastet § 1 bokstav a og e.

De generelle merknadene til begge punkter i første ledd er utførlige og gir liten foranledning til supplering i de spesielle merknadene. Her skal det bare kort konstateres at med «bruk» menes faktiske handlinger og ikke rettslige disposisjoner. Hvorvidt bruken er rettsstridig og rammes av utkastet § 8, må avgjøres på grunnlag av andre lovregler, de retningslinjer som gjelder for bruken av det aktuelle system, kutyme og en bedømmelse av handlemåten sett i forhold til datasystemets formål m.v.

Bruk som forestås av personer som er uberettiget til å skaffe seg tilgang til datasystemet, jf. utkastet § 4, vil rammes av utkastet § 8, selv om bruken gjelder ordinære funksjoner på systemet. Bruk som foretas av personer som har lovlig tilgang til systemet, må vurderes i lys av øvrige regler og retningslinjer som nevnt.

Utkastet § 8 ville kunne anvendes i visse typer «telleskrittsaker». Det vises til kapittel 5.8.7 om dette.

I første ledd annet punkt presiseres det at bruk av en annens tilgangspunkt til internett i usikret trådløst nettverk, ikke anses å være rettsstridig. Det er gitt en utførlig begrunnelse for dette i de generelle merknadene i kapittel 5.6.5 i underkapitlet «Rettsstridsreservasjonen» underpunkt b, og det henvises dit. Regelen reiser ikke spesielle tolkingsproblemer. Det kan dog presiseres at den ikke gjør tilgang til øvrige deler av en annens usikrede datasystem rettmessig. Dette rammes uansett av utkastet § 4.

## 9.9 Utkastet § 9. Etterfølgende befatning med ulovlig data og databasert informasjon m.v.

Utkastet § 9 lyder:

> «For etterfølgende befatning med data og databasert informasjon straffes den som uberettiget benytter, avhender eller tilgjengeliggjør data eller databasert informasjon som er utbytte av en handling som er straffbar etter dette kapitlet.
>
> Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.»

Det vises til merknadene i kapittel 5.5.3.

Straffebudet i utkastet § 9 gjelder etterfølgende befatning med utbytte av straffbar handling og er følgelig beslektet med straffeloven § 317 om heleri, hvitvasking og sikringshandlinger. Utkastet § 9 er en spesialregel som kommer til anvendelse når utbyttet består i «data og databasert informasjon» og stammer fra en handling som er straffbar etter reglene i datakrimkapitlet. Det mest praktiske er at

primærforbrytelsen består i overtredelse av reglene om informasjons- og datatyveri, jf. utkastet §§ 5 og 6, men også data og databasert informasjon som for eksempel anskaffes via elektronisk kartlegging, jf. utkastet § 2, kan være utbytte i utkastet § 9 sin forstand.

Etter gjeldende rett omfattes data og databasert informasjon av utbyttebegrepet i straffeloven § 317, men på grunn av den særegne karakteren av slikt utbytte reiser det seg noen egne problemstillinger hvor det kan være tvilsomt om straffeloven § 317 strekker til. Disse problemstillingene er belyst i kapittel 5.5.3. På grunn av den store økonomiske verdien som ligger i slikt utbytte er det behov for eksplisitt straffehjemmel, jf. utkastet § 9, som følgelig er å anse som *lex specialis* i forhold til straffeloven § 317.

Utkastet § 9 supplerer og presiserer straffeloven § 317 for å skape klar hjemmel for straff for tilfeller som ellers kunne fremstå som tvilsomme. Utkastet § 9 dekker ikke uttrykkelig heleri og hvitvaskingsalternativene i straffeloven § 317 første ledd. Årsaken er at disse reglene ikke ses å reise spesielle spørsmål ved anvendelse på data og databasert informasjon. Ved heleri og hvitvasking er straffeloven § 317 første ledd fortsatt hovedbestemmelsen for data og databasert informasjon.

Tilgangsdata, skadelig dataprogram og selvspredende dataprogram kan også være utbytte av straffbar handling, for eksempel etter fremstillingsalternativet i utkastet §§ 10-12. I utgangspunktet er det meningen at utkastet §§ 10-12 uttømmende regulerer straffbar befatning med slikt utbytte. Alle de nevnte straffebestemmelsene inneholder alternativer i gjerningsbeskrivelsen som omfatter etterfølgende befatning, jf. «anskaffer». Etter de nevnte straffebudene er det (i motsetning til for utkast § 9), ikke noe vilkår at anskaffelsen skjer etter en forutgående primærforbrytelse. Det strafferettslige innslagspunktet settes altså tidligere enn for handlinger som bedømmes etter utkastet § 9. Men området for utkastet § 9 er vidt og det kan derfor oppstå tilfeller hvor straffebudet supplerer utkastet §§ 10-12.

«Data» og «databasert informasjon» i utkastet § 9, er definert i utkastet § 1 bokstav c og d, og det vises til merknadene til disse bestemmelsene.

Utkastet § 9 rammer etterfølgende handlinger enten de er begått av primærforbryteren eller en tredjeperson. I den grad handlingen begås av primærforbryteren, det vil si den som har begått data eller informasjonstyveriet, er straffebudet overlappende med straffeloven § 317 annet ledd. Utkastet § 9 går imidlertid lenger enn til å omfatte sikringshandlinger, idet både endelig realisasjon og endelig utnyttelse av utbyttet for primærforbryterens egen del omfattes. Dette skyldes de særegne hensyn som gjør seg gjeldende for data og databasert informasjon, hvor mulighet for naturalrestitusjon og erstatning kan være begrenset samtidig som den skadelige effekt gjør seg gjeldende for fullt. Det vises til merknadene i kapittel 5.5.3.

De straffbare alternativ etter gjerningsbeskrivelsen er «benytter», «avhender» og «tilgjengeliggjør».

Alternativet «benytter» gjelder det å utnytte utbyttet, for eksempel i sin egen virksomhet. Alternativet omfatter utnyttende handlinger som skjer ikke bare for å skjule utbyttet, men også som en endelig disponering, og også når utnyttelsen skjer av primærforbryteren selv. Det antas at utkastet § 9 her går lenger enn straffeloven § 317 annet ledd.

Alternativet «avhender» omfatter ikke bare sikringshandlinger, men også endelig realisasjon av utbyttet. Også dette alternativet omfatter avhending som begås av primærforbryteren selv, og rekkevidden av utkastet § 9 er dermed også her videre enn straffeloven § 317 annet ledd.

Alternativet «tilgjengeliggjør» omfatter for eksempel at dataene eller den databaserte informasjonen spres via e-post, legges tilgjengelig på en hjemmeside eller sies videre til andre (muntlig overlevering).

## 9.10 Utkastet § 10. Ulovlig befatning med tilgangsdata

Utkastet § 10 lyder:

> «For ulovlig befatning med tilgangsdata straffes den som uberettiget anskaffer, innfører, fremstiller, besitter, markedsfører eller tilgjengeliggjør for andre passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem.
>
> Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen fengsel inntil 3 år.»

Det vises til merknadene i kapittel 5.7.4.

Nøkkelbegrepet er «tilgangsdata» som i bestemmelsen er angitt som «passord, adgangskode, krypteringsnøkkel eller lignende». Av «eller lignende» fremgår det at oppregningen ikke er uttømmende. For å omfattes av bestemmelsen er det videre et vilkår at tilgangsdataene kan gi tilgang til «data, databasert informasjon eller datasystem». Der de gir tilgang til andre objekter enn

angitt i straffebudet faller de utenfor begrepet «tilgangsdata» i utkastet § 10. Praktiske eksempler på tilgangsdata som *ikke* omfattes av utkastet § 10 er slike som anvendes i elektroniske låssystemer til bygninger og biler.

Utkastet § 10 gjelder handlinger som kan inngå i forberedelsen til en handling som er straffbar etter utkastet §§ 4-6. Det er imidlertid ikke nødvendig å bevise at handlingen etter utkastet § 10 hadde som konkret formål å begå, forsøke, eller medvirke til å begå, en slik overtredelse. Det er tilstrekkelig å ha hatt en befatning som angitt i straffebudet med en tilgangskode som nevnt.

Overtredelse av utkastet §§ 4-6, når dette skjer ved rettsstridig bruk av tilgangsdata, kalles passordinnbrudd, eventuelt ulovlig dekoding. Eksempler på denne form for overtredelse av de nevnte straffebud er innlogging på et datasystem eller brukerkonto med et stjålet passord (utkastet § 4), uberettiget dekoding av betalingsbelagte tilgangskontrollerte kringkastingssignaler (utkastet § 5), og maskinell dekryptering av en kryptert passordliste som lagres i en fil med dekrypterte data (utkastet § 6).

I vanlig språkbruk omtales tilgangskoden i entall. Her gis den bokstaven A. Når koden A anvendes for å beskytte data, databasert informasjon eller datasystemer foreligger den imidlertid i to korresponderende representasjoner: A1 og A2. Den ene representasjonen (A1) er anvendt på dataene, den databaserte informasjonen eller på datasystemet. Dette er når data og databasert informasjon er kryptert, og datasystemet er tilgangskontrollert. Den andre korresponderende representasjonen av koden (A2) besittes av en ekstern aktør (person eller datasystem) som må avgi A2 for å oppnå tilgang. Når A2 avgis til systemet vil den gjenkjennes og aksepteres av A1. Dette har med autentiseringsrutinen å gjøre, se kapittel 4.6.2. Begge representasjonene av tilgangskoden kan være gjenstand for de befatningsformer som er angitt i utkastet § 10.

Det er uten betydning i forhold til utkastet § 10, om krypteringssystemet er symmetrisk eller asymmetrisk. Ved symmetrisk kryptering er A1 lik A2. Ved asymmetrisk kryptering er A2 definert ut fra A1, men er i formen ulik A1. Når det ovenfor er sagt at A1 og A2 er korresponderende nøkler, gjøres det ikke noen forutsetning om hvilken krypteringsform som er benyttet. Det sentrale er at A1 er implementert på objektet, mens A2 besittes av den som skal avgi tilgangskoden.

Siden tilgangskodene nevnt i utkastet § 10 anvendes på data, databasert informasjon eller datasystemer, vil A1 alltid være representert som «data» fordi den vil ligge implementert i det objekt den beskytter. Slik sett er uttrykket «tilgangsdata» i utkastet § 10 dekkende. Det er imidlertid ikke noe rettslig vilkår at den korresponderende koden A2 foreligger i form av «data». A2 kan være et passord som en person husker, eller som er skrevet ned på en papirlapp eller som er formidlet muntlig. A2 kan også foreligge som «databasert informasjon» og «data». Lister som verserer på internett med oppdaterte kodenøkler til bruk for piratdekoding av fjernsynssendinger, kan leses og utnyttes av mennesker og er dermed kodenøkler representert som databasert informasjon. Det samme gjelder passordfiler med et innhold som bare kan leses og utnyttes av datamaskiner, for eksempel til å foreta et maskinelt passordinnbrudd i et annet datasystem over internett.

Utover at A1 må være databasert stilles det ikke noe krav til tilgangskodens form. Enhver form for tegnstreng eller digitalisert kjennemerke, som for eksempel et fingeravtrykk, er omfattet.

De straffbare befatningsformer er «anskaffer», «innfører», «fremstiller», «besitter», «markedsfører» eller «tilgjengeliggjør». Disse alternativene dekker alle straffbare befatningsformer som følger av straffeloven § 145 b, straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd og § 53c. Etter straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd kan det ha betydning for straffbarheten om handlingen skjer i vinnings hensikt. Etter lovforslaget er vinningsmomentet en skjerpende omstendighet ved handlingen, jf. utkastet § 18, men ikke en betingelse for straff, jf. utkastet § 10. Det vises ellers til de generelle merknadene om regelharmonisering, se kapittel 5.1.2 med videre henvisninger.

«Anskaffer» betyr å motta noe som følge av at man har utvist en viss aktivitet. Alternativet rammer ikke den som passivt og mer tilfeldig mottar en kode (A2) som man er uberettiget til. Det kreves ikke at man er aktiv hver gang det er aktuelt å motta en kode. Det er for eksempel tilstrekkelig å ha satt seg på en varslingsliste per e-post eller sms hvor man fortløpende mottar nye koder når de gamle skiftes ut av rettighetshaverne. Dette dekkes av anskaffelsesalternativet. Det kreves heller ikke at mottakeren har tatt initiativet til å motta koden. En som på forespørsel aksepterer et tilbud om å motta en slik kode anses å ha anskaffet den i lovens forstand. Ytterligere kan anskaffelse skje ved å videofilme inntasting av passord, eller ved å anvende en tastetrykksavleser. Plasseringen av det utstyr som er nødvendig for å foreta filmingen eller registreringen av tastetrykkene er straffbar etter utkastet § 3, mens igangsetting av filming eller av

tastetrykksregistratoren (dersom denne betjenes på distanse) rammes av utkastet § 10. Hvis man ikke lykkes i å tolke tastetrykkene foreligger det forsøk på anskaffelse av tilgangskoder.

«Innfører»: Dette alternativet dekker den tilsvarende formulering i gjeldende bestemmelser i straffeloven § 262 første ledd bokstav a, og åndsverkloven § 53a annet ledd bokstav b, og er nødvendig først og fremst for å sørge for at de folkerettslige forpliktelser etter de nevnte bestemmelsene er oppfylt. Alternativet rammer den som anskaffer tilgangsdata over landegrensene. Som oftest vil nok handlingen kunne henføres under anskaffelsesalternativet, for eksempel ved formidling av koder på internett hvor det neppe er nærliggende å tenke at det foreligger innførsel selv om man mottar eller henter dataene fra et utenlandsk nettsted. For et tilfelle fra rettspraksis kan det vises til Rt. 1995 side 1872 (pinkodekjennelsen), hvor domfelte hadde mottatt en pinkode fra en israeler via en elektronisk oppslagstavle, det vil si en tidlig internettjeneste. Men dersom man mottar et brev fra utlandet inneholdende slike tilgangsdata som utkastet § 10 nevner, er kravet til innførsel oppfylt.

«Fremstiller» omfatter det å gjøre en egen innsats for å avdekke eller gjette passord og kodenøkler. Alternativet omfatter for eksempel passordknekking. Passordknekking maskinelt utført er gjetting av passord, enten ordlistebasert (dictionary attack) eller ved vilkårlig gjetting (brute force /«rå kraft»). Disse fremgangsmåtene er også beskrevet i kapittel 3.4.7. Ytterligere rammes menneskelig gjetting av passord, slik som når man tenker seg hva den berettigete har satt som passord.

Ved menneskelig gjetting av passord kan det reises spørsmål ved om passordet må være testet for å anses «fremstilt». Hvis ikke vil det være straffbart å gjette passord på ren intuisjon, noe som kan synes å gi straffehjemmelen en noe vid slagvidde. Rettsstridsreservasjonen begrenser imidlertid regelens rekkevidde i disse tilfellene, idet det ikke kan være rettsstridig å gjette eller tenke på andres passord. Passordet må følgelig være verifisert for å anses «fremstilt» etter utkastet § 10. Dersom verifikasjon må skje på et system man ikke er berettiget til å benytte, vil testing også innebære en overtredelse av utkastet § 4. Det kunne dermed synes å være tilstrekkelig med straff for den ulovlige tilgang, eller forsøket på dette, fremfor å anvende utkastet § 10. Denne lovforståelsen fanger imidlertid ikke opp de tilfelle hvor lovovertrederen avbryter testingen så tidlig at kravet til «tilgang» etter utkastet § 4 ikke kan anses oppfylt. Den vil heller ikke fange opp tilfeller hvor lovovertrederen tester passord, ikke for å benytte dem selv, men for å spre dem videre. I slike tilfelle vil neppe kravet til forsett om uberettiget tilgang til datasystem være oppfylt, jf. utkastet § 4.

Maskinell passordknekking inneholder en verifikasjonsprosedyre, så her er det tilstrekkelig for straff å bevise at passordknekkingen gjelder passord som kan gi tilgang til data, databasert informasjon eller datasystem.

Andre tilfeller av menneskelig tilegnelse av passord som omfattes av fremstillingsalternativet, er der hvor lovovertrederen analyserer opplysninger med tanke på å avdekke kamuflerte passord, for eksempel pinkoder som er forsøkt kamuflert i kombinasjon med andre numre. For et eksempel fra rettspraksis vise det til Rt. 2004 side 499, hvor kodene var forsøkt kamuflert i sammenstilling med fødselsdatoer (dommens avsnitt 35). Selve den anstrengelsen som ligger i analysen av telefonnummeret innebærer at kravet til fremstilling er oppfylt, når man har forstått koden. Det kreves ikke testing i tillegg. Alternativt vil handlingen kunne rammes av anskaffelsesalternativet, det vil si ved at man har anskaffet de kamuflerte kodene. Dermed er handlingen fullbyrdet allerede ved anskaffelsen, det vil si før den etterfølgende analysen (fremstillingen). Dette antas også å gi det klareste skjæringspunktet for fullbyrdet handling i disse tilfellene.

Fremstilling omfatter også avdekking av tilgangskoder som skjer som del av en analyse av et dataprogram. Det vises til de generelle merknadene om dette i kapittel 5.7.4, hvor det er lagt til grunn at lovlig analyse av dataprogram ikke nødvendigvis gjør avdekking av tilgangskoder som ligger skjult i programmet, lovlig. Analysen må med andre ord legges opp slik at den respekterer kodekonfidensialiteten. Hvis dette ikke er mulig for å gjennomføre analysen og denne ellers ikke er rettsstridig, vil neppe heller fremstillingen av tilgangskoden være rettsstridig. Dette må vurderes konkret i det enkelte tilfellet, hvor formålet med analysen må stå sentralt. Går analysen ut over det som følger av formålet med den følge at tilgangskoder avdekkes, vil det kunne være å anse som rettsstridig fremstilling av tilgangsdata.

«Besitter» betyr å ha tilgangsdataene på et sted man selv kontrollerer. Besittelsens karakter er uten betydning. Det kan for eksempel være at passord m.v. er skrevet ned for hånd, eller ligger lagret på et brukerområde på en lokal datamaskin eller på et nettsted på internett, som man selv kontrollerer. Det er uten betydning om nettstedet er på en norsk eller utenlandsk server, eller om tjenesteyteren er norsk eller utenlandsk, så lenge tilgangsdataene

oppbevares under lovovertrederens direkte kontroll, eventuelt etter vedkommendes instruks.

Besittelsesalternativet vil også ramme tilfeller hvor besittelsen har oppstått uforsettlig, men hvor besitteren unnlater å slette tilgangskodene etter at han ble oppmerksom på besittelsen. Dette kan være aktuelt med tanke på besittelse som har oppstått på unnskyldelig vis som følge av lovlig analyse av dataprogram, se ovenfor. Men når vedkommende blir klar over at analysen har avdekket tilgangskoder oppstår en umiddelbar slettingsplikt for å unngå å bli rammet av besittelsesalternativet.

«Markedsfører» betyr å tilby eller reklamere for spredning av tilgangsdata. Som eksempel rammes det å tilby hyperlenker til nettsteder som formidler tilgangsdata, av dette alternativet. Det er ikke noe vilkår at markedsføringen skjer som ledd i økonomisk virksomhet eller med økonomisk motiv.

«Tilgjengeliggjør» dekker enhver form for spredning av tilgangsdata. Det kan være spredning via internett fra en til en, eller fra en til mange for eksempel via en hjemmeside, på nyhetsgrupper eller pratekanaler. Spredning kan ellers skje muntlig, formidles skriftlig på papir osv. Tilgangskoder som er implementert i dataprogram eller piratdekoderkort m.v., kan spres som følge av at programmet eller kortet spres. Spredningen av dataprogrammet DeCSS som inneholdt tilgangskode for å dekryptere den elektroniske beskyttelsen på dvd-filmer, er et eksempel på dette, se RG 2004 side 414 (dvd-dommen). Slike indirekte spredning av tilgangskoder rammes ikke av utkastet § 10, men av utkastet § 11.

Blant de mange praktisk tenkelige tilfelle av spredning av tilgangsdata, inngår spredning som skjer etter at man eventuelt er kommet i besittelse av tilgangsdata som følge av analyse av dataprogram, jf. de foregående bemerkningene om dette. For det første oppstår slettingsplikt for å unngå straffansvar etter besittelsesalternativet. Hvis tilgangsdataene i tillegg spres, er det straffbart etter tilgjengeliggjøringsalternativet.

## 9.11 Utkastet § 11. Skadelig dataprogram og utstyr

Utkastet § 11 lyder:

> «For ulovlig befatning med skadelig dataprogram straffes den som uberettiget anskaffer, fremstiller, modifiserer, besitter, markedsfører eller tilgjengeliggjør dataprogram som er særlig egnet til å begå handlinger som er straffbare etter §§ 4-8, 10 eller 13-14 i dette kapitlet. Liknende befatning med utstyr som er særlig egnet til tilsvarende formål straffes på samme måte.
>
> Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.»

Det vises til kapittel 5.7 og datakrimkonvensjonen artikkel 6.

Bestemmelsen rammer befatning med skadelig dataprogram og utstyr. Som det fremgår foran, er denne bestemmelsen foreslått under dissens. Lovmotivene her omhandler flertallets forslag. For mindretallets syn, henvises det til kapittel 5.7. Forslaget innebærer en kriminalisering av innledende handlinger som generelt ikke tidligere har vært straffbar. Flertallet mener at dette vil ha en normskapende og en forebyggende effekt. Bestemmelsen gir muligheter for inngrep før det er begått handlinger som gir direkte skadevirkninger i forhold til konkrete fornærmede.

Første ledd første punktum gjelder skadelig dataprogram. Som skadelig dataprogram regnes dataprogram som er særlig egnet til å begå visse straffbare handlinger. Dette gjelder konkret handlinger som rammes av datakapitlets §§ 4-8, 10 eller 13-14. Dette innebærer at blant annet programmer som er særlig egnet til å bli benyttet for å skaffe seg ulovlig tilgang til et datasystem omfattes av bestemmelsen. Dette er for eksempel såkalte exploits, som er beregnet på å utnytte sårbarheter i programmer som kjøres på et datasystem. Det samme gjelder programmer som er særlig egnet til å begå datatyveri, informasjonstyveri, datamodifikasjon eller uberettiget bruk av andres datasystem. Likedan omfattes dataprogram som er særlig egnet til å ha ulovlig befatning med tilgangsdata, program som er særlig egnet til å forårsake driftshindring og program som er særlig egnet til å foreta ulovlig masseutsendelse av elektroniske meldinger.

Programmer som er særlig egnet til å bli benyttet ved andre handlinger som er straffbare etter datakrimkapitlet, omfattes ikke av utkastet § 11. Dette gjelder for eksempel programmer som er særlig egnet til å foreta elektronisk kartlegging av datasystem. Grunnen til at enkelte av straffebudene har vært holdt utenfor oppregningen, er enten at slike programmer kan ha så mange nyttige formål at utvalget har veket tilbake for å straffbelegge befatning med dem, eller at det antas lite praktisk med bruk av dataprogrammer i forbindelse med lovbruddet. Det første er tilfelle i forhold til utkastet § 2, og det siste er tilfelle i forhold til utkastet § 9.

Programmer med selvspredende egenskaper straffes etter utkastet § 12. Programmer med selvspredende egenskaper regnes derfor ikke som skadelige programmer etter utkastet § 11. Selvspredende dataprogrammer kan, i tillegg til at de er selvspredende, også inneholde egenskaper som i utgangspunktet faller inn under utkastet § 11. I disse tilfellene er imidlertid ikke § 11 og § 12 tenkt anvendt i konkurrens. Meningen er at også andre skadelige egenskaper enn de selvspredende konsumeres av utkastet § 12. Dette fremgår av utkastet § 12 fjerde ledd annet punktum, som utvider strafferammen i slike tilfeller.

Annet ledd likestiller skadelig utstyr med skadelig dataprogram. Dette gjelder for eksempel utstyr som kan utplasseres for ulovlig å registrere tastetrykk for å fange opp informasjon, herunder passord, hos tredjemann (såkalt tastetrykkregistrator eller «key stroke logger»).

Det er et vilkår for straffbarhet at dataprogrammene eller utstyret er «særlig egnet» til å begå de spesifiserte straffbare handlingene. Programmer og utstyr kan benyttes i mange sammenhenger og til mange formål. Noe som er utviklet og vanligvis benyttes til helt legitime formål, kan i enkelte sammenhenger også bli benyttet til straffbare formål. Omvendt kan noe som er utviklet til bruk ved straffbare handlinger også benyttes til lovlige formål. Etter forslaget må objektet være særlig egnet til å begå de nevnte handlingene. Meningen med dette er at det skal være en høy terskel for når program eller utstyr faller inn under utkastet § 11. Det er ikke hensikten å ramme ellers lovlige programmer og utstyr selv om de også i visse tilfeller vil kunne benyttes til straffbare handlinger. Hensikten er å straffbelegge befatning med programmer og utstyr som i første rekke er utviklet eller anskaffet med tanke på å begå straffbare handlinger eller som har sin viktigste funksjon i denne sammenheng.

Verktøyet kan ha en slik karakter at det kan utnyttes alene eller sammen med andre komponenter. Det betyr at utkastet § 11 omfatter den praktiske situasjon at det spres verktøy som i tillegg må kodes for å kunne begå den straffbare handling. Det kan være tale om blanke kort, for eksempel magnetstripekort eller smartkort, som må kodes for å kunne benyttes til å oppnå tilgang til et datasystem eller fjernsynssignaler. At dette er praktisk illustreres blant annet ved noen eksempler fra rettspraksis, se Smartkortdommen (Rt. 1995 side 35) hvor gjerningspersonene solgte piratdekodekort som kunne dekode betalingsbelagte fjernsynssignaler. Det kan også vises til Nedenes herredsretts dom av 1. juli 1998 hvor domfelte hadde solgt blanke smartkort til kunder som ønsket å foreta «piratdekoding» av fjernsynssignaler. I tillegg distribuerte han informasjon om kodene som kunne benyttes på kortene, og i visse tilfeller utførte han også selve kodingen. Poenget er at brukeren gjerne trenger både det fysiske utstyret og tilgangskodene. Utstyret blir rammet av utkastet § 11 uansett om det er kodet eller ikke. Vernet om kodene isolert sett følger av utkastet § 10.

Det er videre et vilkår for straffbarhet at befatningen er urettmessig. Den som har befatning med et skadelig program for lovlige formål, handler ikke urettmessig. Dette vil være tilfelle hvis vedkommendes befatning med objektet har sammenheng med lovlig bruk vedkommende gjør eller har planlagt å gjøre med objektet. Befatning med et spamprogram vil for eksempel være rettmessig hvis det er ment brukt til lovlig utsendelse til medlemmene i en forening eller kundene til et firma, men ikke hvis det er ment brukt til ulovlig masseutsendelse. Befatning med objektet vil også være lovlig hvis det skjer som ledd i forskning eller utvikling av sikkerhetsprodukter. I denne sammenheng er det ikke nødvendig at den som har befatning med objektet har en formell forskerstatus, men det kan ha betydning ved bevisvurderingen. Som ellers i strafferetten er det påtalemyndigheten som må føre bevis for at tiltaltes befatning med objektet er urettmessig, men det antas at de konkrete omstendighetene i den enkelte sak vil gi nødvendig veiledning.

Skyldformen er forsett. Det kreves at forsettet omfatter selve befatningen med objektet og objektets skadelige egenskaper. Dessuten må forsettet også omfatte de elementer som gjør befatningen med objektet urettmessig. Uaktsom overtredelse av § 11 er ikke foreslått gjort straffbar, jf. utkastet § 17. Grunnen til dette er at det i disse tilfellene vil bli for strengt å ramme uaktsomhet. Det er for eksempel fort å komme i besittelse av et objekt i slike tilfeller uten at en tenker over de ulike bruksmulighetene for objektet.

De straffbare befatningsformene er anskaffelse, fremstilling, modifisering, besittelse, markedsføring og tilgjengeliggjøring. Med fremstilling menes det at lovbryteren selv utvikler programmet eller lager utstyret. Modifisering tar sikte på at lovbryteren endrer et program eller utstyr som er utviklet eller bygget av andre. Det har ikke betydning om det opprinnelige objektet rammes av utkastet § 11. Med anskaffelse menes at vedkommende skaffer seg objektet. Det er uten betydning om det ytes vederlag. Anskaffelse kan for eksempel skje ved nedlasting fra internett. Anskaffelsen

må skje forsettlig. Det er ikke straffbart om man uten å tenke over det mottar programmet i tilknytning til et selvspredende program eller som en del av en samlet programvare som installeres.

Også besittelse er foreslått gjort straffbart. Besittelse vil for eksempel foreligge dersom lovbryteren har programmet lagret på sitt datasystem. Besittelsen må i tilfelle være forsettlig, og forsettet må her som ellers omfatte alle straffbarhetsvilkårene.

Også markedsføring og tilgjengeliggjøring av skadelig programvare er foreslått omfattet av bestemmelsen. Tilgjengeliggjøring foreligger for eksempel dersom et skadelig dataprogram legges ut på internett for nedlasting; enten gratis eller mot vederlag. Det samme gjelder ved direkte salg av objektet. Markedsføring grenser nær opp til tilgjengeliggjøring, og alternativene kan av og til være overlappende. Med markedsføring tenker en dog vanligvis på en noe mer oppsøkende tilnærming mot potensielle brukere, for eksempel i form av annonsering.

Utkastet § 11 vil i mange tilfeller kunne benyttes i konkurrens med andre straffebud i utvalgets forslag. Har en lovbryter utviklet et programverktøy for inntrengning i andres datasystemer og vedkommende senere benytter dette verktøyet til inntrengning, kan utkastet § 11 og § 4 benyttes i realkonkurrens. Utkastet § 11 og § 12 er imidlertid ikke ment benyttet i konkurrens, slik det er gjort rede for ovenfor i dette kapitlet.

Utvalget har gått inn for å samordne datakrimkapitlet med straffeloven § 262. Dette innebærer at § 262 første ledd videreføres gjennom straffebudet i utkastet § 11.

Et flertall i utvalget har gått inn for å samordne datakrimkapitlet med enkelte bestemmelser i åndsverkloven. Det vises til kapittel 5.1.2, 5.5.2 og 5.6.2. Det ligger i dette flertallets forslag at også bestemmelsene i åndsverkloven § 53a annet ledd og § 53c videreføres gjennom utkastet § 11.

Strafferammen er foreslått satt til bøter eller fengsel inntil ett år. Dessuten er det foreslått en egen bestemmelse om grov overtredelse hvor strafferammen er bøter eller fengsel inntil tre år.

## 9.12 Utkastet § 12. Spredning av selvspredende dataprogram

### 9.12.1 Innledning

Utkastet § 12 lyder:

> «For ulovlig befatning med selvspredende dataprogram straffes den som uberettiget fremstiller, modifiserer, anskaffer eller tilgjengeliggjør selvspredende dataprogram.
>
> For ulovlig befatning med selvspredende dataprogram straffes også den som initierer spredning av slikt program.
>
> Med selvspredende dataprogram menes dataprogram som kan videredistribuere seg til andre datasystemer og installeres automatisk eller ved at noen foretar eller godkjenner installasjonen uvitende om dataprogrammets selvspredende egenskaper.
>
> Straffen er bøter eller fengsel inntil 1 år. Inneholder det selvspredende dataprogrammet også andre skadelige egenskaper er straffen bøter eller fengsel inntil 3 år. For grov overtredelse er straffen bøter eller fengsel inntil 6 år.»

Det vises til merknadene i kapittel 5.7.6.

Straffebudet rammer befatning med selvspredende dataprogram. Første og annet ledd angir de straffbare befatningsformer. Tredje ledd inneholder en legaldefinisjon av selvspredende dataprogram. Fjerde ledd angir differensierte strafferammer ved overtredelse, blant annet for å ta hensyn til andre skadelige egenskaper ved dataprogrammet.

De legislative hensyn bak straffebudet er at selvspredende dataprogram forårsaker belastninger i det elektroniske kommunikasjonsnettet og på de datasystem som infiseres (vertsmaskinene). Selvspredende dataprogram utgjør en stor trussel mot hensynet til systemintegriteten, jf. kapittel 4.6.2. Videre representerer selve infiseringen en form for ulovlig tilgang og datamodifikasjon, samt at det kan lede både til konfidensialitetskrenkelser og driftshindring. Utkastet § 12 har derfor slektskap med utkastet §§ 4, 7 og 13, og støtter seg dessuten til dels på tilsvarende legislative hensyn som utkastet § 14.

### 9.12.2 Selvspredende dataprogram – legaldefinisjonen i utkastet § 12 tredje ledd

Selvspredende dataprogram er definert i utkastet § 12 tredje ledd. Definisjonen består av to ledd, se nedenfor. Grunnbetingelsen er at det er tale om et «dataprogram», jf. utkastet § 1 bokstav b. Dette innebærer krav om at innholdet i dataene er slik at de gir instruksjon til et datasystem. Definisjonen omfatter dataprogram som er ferdig kompilert og følgelig er i en form som gjør at det kan påvirke funksjoner og instruere det datasystem som aktiviserer programmet. Definisjonen omfatter også kildekode, det vil si dataprogram som foreligger som en programmeringstekst og som må kompileres for å kunne installeres på datasystemet. Kompilering er en maskinell konverteringsprosess fra

kilde- til objektkode, som enkelt utføres ved hjelp av et dataprogram. Legaldefinisjonen av selvspredende dataprogram omfatter dataprogram både som kilde- og objektkode (og eventuelle mellomformer som assemblykode). Det vises til eksemplifiseringen nedenfor i forbindelse med de straffbare befatningsformer.

Etter første ledd i definisjonen kreves det at det er tale om «dataprogram som kan videredistribuere seg til andre datasystemer». Dette innebærer som det fremgår, et krav om at dataprogrammet har slik funksjonalitet at det kan foreta selvspredning til andre datasystemer. Av «kan videredistribuere seg» fremgår det at det er egenskapen ved programmet som har betydning, ikke om videredistribusjon faktisk har skjedd. Dette vilkåret kan være oppfylt uavhengig av programmets form for øvrig, det vil si uavhengig av om det foreligger i objekt- eller kildekode.

Uttrykket «videredistribuere seg» er sentralt fordi det gir anvisning på at viderespredning skjer uten noen innsats eller handling forøvrig av et menneske. Viderespredning skjer følgelig utelukkende som følge av programmets egenskap og utenfor menneskelig styring og kontroll.

Det kreves også at selvspredningsformen er slik at programmet «kan» spre seg selv til «andre datasystemer». Dersom programmet har slik funksjonalitet at det kopierer seg selv på det samme datasystemet, er det ikke et selvspredende dataprogram, slik begrepet er definert i utkastet § 12 tredje ledd, men et *skadelig* program som forårsaker datamodifikasjon eller ulovlig bruk av et datasystem, jf. utkastet §§ 7 og 8. Befatningen skal i så fall bedømmes etter utkastet § 11. Dersom programmets selvspredningsfunksjonalitet er slik at det kopierer seg til lagringsmedier som naturlig flyttes mellom datasystemer, for eksempel til en cd-plate eller til en minnepinne, anses vilkåret «kan» spre seg til «andre datasystemer» å være oppfylt.

For det annet kreves det at programmet «installeres automatisk eller ved at noen foretar eller godkjenner installasjonen uvitende om dataprogrammets egenskaper». Dette leddet i definisjonen består av to alternativ hvorav minst ett må være oppfylt i tillegg til definisjonens første ledd som er beskrevet i det foregående.

Første alternativ i dette definisjonsleddet er «installeres automatisk». Vilkåret gir anvisning på at dataprogrammet legger seg på vertsmaskinen uten at det kreves noen aksepterende handling på dennes vegne. Blant annet har såkalte «ormer» denne egenskapen. Videre kan det selvspredende programmet ha blitt lagt tilgjengelig på en hjemmeside og installert seg automatisk på de datasystem som har kontaktet hjemmesiden. Det kan også være lagt ut i et fildelingssystem, på en samtaletjeneste eller i et tekstmeldingssystem, og så smitter det automatisk videre fra de datasystem som er infisert til de øvrige som kommuniserer med dem.

Annet alternativ i dette definisjonsleddet gjelder «at noen foretar eller godkjenner installasjonen uvitende om dataprogrammets egenskaper». Alternativet omfatter dataprogram som sprer seg selv, men som krever aksept fra mottaker for å bli installert på vertsmaskinen. Dette alternativet innebærer et element av forledelse, jf. vilkåret «uvitende om dataprogrammets egenskaper». Mottaker blir altså forledet til å la sin maskin infisere av et selvspredende dataprogram og således bli en plattform for viderespredning, det vil si forårsake fortsatt skadeforvoldelse i nettet. Dette definisjonsleddet forutsetter derfor at dataprogrammet er slik laget at det fremstår som en legitim fil. Det er imidlertid ikke noe vilkår at det fremstår som et *program*, og selvsagt heller ikke at det har selvspredende funksjonalitet. Det er tilstrekkelig at det for eksempel er et vedlegg til en e-post hvor man oppfordres til å åpne vedlegget, for eksempel for å motta en hilsen eller et godt tilbud. Dermed installeres programmet som ligger i vedlegget. Vedlegget inneholder med andre ord et aktivt program som blir kjørt på datamaskinen uten at mottaker forstår det når vedkommende åpner vedlegget. Deretter fortsetter programmet å spre seg selv via e-posttjenesten på den infiserte maskin. Det å åpne vedlegget er en aksept i utkastet § 12 tredje ledds forstand.

En annen variant kan være at en tilsynelatende ordinær programfil, for eksempel for en fildelingstjeneste som lastes ned på internett, også inneholder selvspredende egenskaper som det ikke opplyses om i sluttbrukeravtalen som man bes om å akseptere. Også denne varianten omfattes av legaldefinisjonen. Legaldefinisjonen krever ikke at dataprogrammet har noen annen skadelig egenskap enn at det er selvspredende. Det vil imidlertid ofte være tilfelle, jf. de generelle merknadene om dette, se kapittel 5.7.6. Dette har betydning for strafferammen, se nedenfor.

### 9.12.3 De straffbare befatningsformer, jf. utkastet § 12 første og annet ledd

De straffbare befatningsformer beskrevet i første ledd omfatter «fremstiller». «modifiserer», «anskaffer» eller «tilgjengeliggjør» Etter annet ledd rammes det å initiere spredning av selvspredende dataprogram.

Alternativet «fremstiller» betyr å lage selvspredende dataprogram, det vil si å programmere et

slikt. Fremstillingsalternativet er fullbyrdet allerede ved fremstilling av kildekoden, det kreves ikke at programmet er kompilert i tillegg slik at det rent faktisk kan installeres på et datasystem. Begrunnelsen ligger i straffebudets preventive formål. Den vesentligste innsatsen bak eksistensen av et selvspredende dataprogram er selve programmeringen. Uten slik skadelig programmeringsvirksomhet hadde selvspredningsproblemet vært vesentlig redusert, om ikke helt borte. Via kildekoden kan også andre få kunnskap om hvordan et selvspredende program kan lages, slik at skadelig programmeringskompetanse spres. Selve kompileringen av kildekoden til objektkode er nødvendig for å iverksette selvspredning, fordi først da kan datasystemet instrueres om å bidra til viderespredningen. Men kompilering er en rask og enkel prosess, og terskelen for å gjennomføre kompilering er lav når kildekoden først foreligger.

Dersom kildekoden inneholder funksjoner for selvspredning er overtredelsen som nevnt fullbyrdet. Men dersom det ved testing i form av objektkode viser seg at selvspredningseffekten ikke inntrer (det er feil i programmet), foreligger bare straffbart forsøk. I fremstillingsfasen er det også praktisk med medvirkningsansvar, for eksempel at en bidrar med råd og veiledning mens en annen utfører den konkrete programmering.

Etter ordlyden omfattes også det å kopiere et selvspredende dataprogram av fremstillingsalternativet, men det antas at anskaffelsesalternativet vil være mer aktuelt i slike tilfelle.

Alternativet «modifiserer» omfatter det å endre et selvspredende dataprogram. En variant kan være å foreta en endring i den delen av dataprogrammet som er gitt en elektronisk signatur. Signaturen anvendes i antivirusfilter og ved å foreta en slik endring vil viruset skifte karakter og ikke bli fanget opp (gjenkjent) i filteret. I realiteten foreligger dermed et nytt virus. En annen variant kan være å bygge ut egenskapene i et selvspredende dataprogram med andre skadelige egenskaper i tillegg, for eksempel gi det funksjonalitet for gjentakende restarting som kan skape driftshindring (bakterieprogram), se kapittel 5.7.6 med videre henvisninger.

Alternativet «anskaffer» omfatter det å aktivt motta et selvspredende dataprogram. Anskaffelsen kan gjelde både kilde- og objektkode. Det preventive formålet med straffebudet tilsier at slik anskaffelse straffes når det skjer frivillig, men det kreves mer enn at man for eksempel har unnlatt å anvende antivirusprogram. Anskaffelse øker risikoen for uønsket viderespredning og kan dessuten spre skadelig programmeringskompetanse. Se merknadene om dette i tilknytning til fremstillingsalternativet, som gjelder tilsvarende her.

Alternativet «tilgjengeliggjør» rammer spredning av selvspredende dataprogram uavhengig av om det er aktivisert eller ei. «Tilgjengeliggjør» rammer følgelig det å gi kildekode til et selvspredende dataprogram videre til en annen. Videre rammes det å spre slikt program i objektkode, selv om det ikke er startet opp (aktivisert). Et eksempel kan være at gjerningspersonen deler dataprogrammet med bekjente, for eksempel ved å kopiere og spre det via cd-rom eller via kommunikasjonstjenester på internett. Ytterligere omfatter tilgjengeliggjøringsalternativet det å legge ut et aktivisert selvspredende dataprogram på en slik måte at andre blir infisert av det, for eksempel ved at programmet er lagt tilgjengelig på en hjemmeside og infiserer de maskiner som kontakter den. Det samme gjelder annen form for spredning, for eksempel som vedlegg til e-post, eller som en aktivisert komponent i et ellers tilsynelatende legitimt dataprogram som startes opp fra en cd-plate (dermed startes også dataviruset).

Tilgjengeliggjøring har en grense mot initiering av spredning, jf. utkastet § 12 annet ledd. Initieringsalternativet rammer den som starter opp et selvspredende dataprogram og følgelig aktiviserer de selvspredende egenskaper. De kan være at samme person først initierer programmet og i tillegg legger til rette for viderespredning ved å legge det ut på sin hjemmeside i aktiv form. Da er både initerings- og tilgjengeliggjøringsalternativet overtrådt.

I praksis vil nok initieringsalternativet være kombinert med tilgjengeliggjøring, men det motsatte er ikke nødvendigvis tilfelle. Det kan være at gjerningspersonen har mottatt et datavirus som allerede er aktivisert, og forsettlig sørger for videre-spredning, for eksempel ved å tilgjengeliggjøre det i enda større grad enn det som ville vært en vanlig følge av selvspredningen, for eksempel ved å brenne det til cd-er som han sprer videre.

Initiering er straffbart også i sin grovt uaktsomme form, jf. utkastet § 17. Det vises til merknadene i kapittel 6.1.

## 9.13 Utkastet § 13. Driftshindring

### 9.13.1 Innledning

Utkastet § 13 lyder:

> «For driftshindring straffes den som uberettiget overfører data under slike omstendigheter at overføringen vesentlig hindrer eller er egnet til vesentlig å hindre driften av et datasystem

eller elektronisk kommunikasjonsnett. Det samme gjelder den som initierer dataoverføring som nevnt.

For driftshindring straffes også den som på annen måte uberettiget foretar handling som er egnet til vesentlig å hindre driften av et datasystem eller elektronisk kommunikasjonsnett.

Straffen er bøter eller fengsel inntil 6 år. For grov overtredelse er straffen bøter eller fengsel inntil 10 år. For liten overtredelse er straffen bøter eller fengsel inntil 1 år.»

Det vises til merknadene i kapittel 5.6.4.

Straffebudet gjelder driftshindring, det vil si handlinger som skader datasystemets eller det elektroniske kommunikasjonsnettets tilgjengelighet. Et annet ord for denne type krenkelse er tjenestenekt. Utkastet § 13 første ledd gjelder logisk angrep som foretas over det elektroniske kommunikasjonsnettet og som leder til driftshindring av et datasystem eller elektronisk kommunikasjonsnett. Utkastet § 13 annet ledd rammer driftshindring som skapes ved at man på annen måte iverksetter kapasitetskrevende prosesser på datasystemet eller det elektroniske kommunikasjonsnettet. Annet ledd tar dermed først og fremst sikte på å ramme tjenestenekt som foretas innenfra det datasystem som utsettes for krenkelsen.

Straffebudet rammer slike skadevoldende handlemåter som utføres ved misbruk av ordinære funksjoner på et datasystem. For handlingene i første ledd fremgår dette av formuleringene «overfører data» (første punktum) og «initierer dataoverføring» (annet punktum). Handlingen i annet ledd er beskrevet som «på annen måte uberettiget foretar handling som er egnet til vesentlig å hindre driften av et datasystem eller elektronisk kommunikasjonsnett». Også dette tar sikte på krenkelse av logisk art. Formuleringene innebærer at fysiske handlinger som krenker tilgjengeligheten ikke omfattes av utkastet § 13. Slike handlinger må i så fall rammes av de alminnelige regler om fysisk skadeverk.

Etter første ledd er det et vilkår at det skadelige resultatet – driftshindringen - fremkalles som følge av dataoverføringen, det vil si av den eksterne påvirkningen som utføres over det elektroniske kommunikasjonsnettet.

Dette avgrenser området for første ledd i forhold til straffebud som rammer det å foreta endringer på et datasystem. Også slike endringer kan lede til driftshindring, men i så fall står man overfor et tilfelle av datamodifikasjon (en uberettiget endring av data på datasystemet), jf. utkastet § 7. Etter utkastet § 7 er driftshindring som følge av en uberettiget endring av data, et moment som kan lede til at handlingen er grov, jf. alternativet «skade som er voldt» i utkastet § 18, og uansett er det et skjerpende moment i straffutmålingen. Det vises også til de generelle bemerkningene om forholdet mellom tilgjengelighets- og integritetskrenkelser i kap. 4.6.2.

Utkastet § 13 annet ledd gjelder handling som innebærer et misbruk av datasystemets funksjoner. Dette reiser visse konkurrensspørsmål i forhold til utkastet §§ 7, 8 g 11, og det vises til merknadene i kapittel 5.6.4. Det vises også til drøftelsen om utkast § 8 nedenfor i kapittel 9.13.4.

Driftshindring er betegnelsen på det skadelige resultatet av handlingen. Det kreves ikke at driftshindringen er absolutt. Dette fremgår av formuleringen «vesentlig» hindrer. Det som kreves er et markert avvik fra datasystemets eller det elektroniske kommunikasjonsnettes ordinære yteevne.

### 9.13.2 Nærmere om utkastet § 13 første ledd

Utkastet § 13 første ledd inneholder tre alternativ, nemlig å foreta handling som resulterer i driftshindring, å foreta handling som er egnet til å resultere i driftshindring, og «å initiere» handling som nevnt.

Selve handlingen som er felles for de tre alternativene, er å overføre data. Objektet for dataoverføringen, det vil si målet for handlingen, er «datasystem» eller «elektronisk kommunikasjonsnett». Disse begrepene er definert i utkastet § 1 bokstav a og e, og det vises til merknadene til definisjonene i kapittel 9.1.

Det følger av dette at metoden må gå ut på å overføre data via et elektronisk kommunikasjonsnett, jf. sammenhengen med definisjonen av «data», jf. utkastet § 1 bokstav c. Det å lamme et datasystem ved hjelp av ekstern stråling rammes dermed ikke av bestemmelsen. Ellers er gjerningsbeskrivelsen utformet slik at den skal være dekkende både for kjente former for overbelastningsangrep (som for eksempel tjenestenektangrep, se kapittel 3.4.9) og mulig fremtidig skadelig metodebruk som setter datasystemer eller elektroniske kommunikasjonsnett ut av funksjon. Begrensningene ligger i at handlingen må foregå over elektronisk kommunikasjonsnett, og at den ikke primært er utført som en integritetskrenkelse, jf. utkastet § 7. Se merknadene om forholdet mellom bestemmelsene i kapittel 5.6.4.

Formuleringen «under slike omstendigheter» innebærer krav om kausalitet, dvs. at egenskaper ved dataoverføringen leder til driftshindringen. Dataoverføringen kan for eksempel være innrettet slik at det sendes for mange eller for ressurskre-

vende datapakker slik at det mottakende datasystem og elektroniske kommunikasjonsnettet inn til systemet, ikke klarer å håndtere dem. Etterhvert fremkalles driftshindring fordi kapasiteten forbrukes til å håndtere dataoverføringen og det blir for lite kapasitet til de ordinære prosesser. Driftshindringen trenger som nevnt ikke være absolutt.

Det kan være at driftshindring ikke inntreffer fordi innehaveren av datasystemet som angripes klarer å beskytte seg mot det skadelige resultatet. Dette har ikke betydning for straffeskylden. Avgjørende er at handlingen er «egnet til» å fremkalle driftshindring. Hvorvidt dette vilkåret er oppfylt beror på en objektiv vurdering hvor man tenker seg effekten av handlingen dersom beskyttelsestiltak ikke hadde vært iverksatt.

Etter annet punktum er den straffbare handling «initierer dataoverføring som nevnt.» Dette skal fange opp de tilfeller hvor gjerningspersonen har etablert et uautorisert nett ved å ha lagt inn dataprogram på fremmede datamaskiner som i sin tur skal benyttes som redskap i utførelsen av et såkalt «distribuert DoS-angrep» mot et tredje datasystem. Gjerningspersonen kan ha gjort alt som er nødvendig for å gjennomføre et angrep ved å ha gitt instrukser til det dataprogrammet som styrer angrepet via det uautoriserte nettet. I et slikt tilfelle er angrepet «initiert», og det foreligger en fullbyrdet overtredelse av utkastet § 13 første ledd annet punktum.

### 9.13.3 Nærmere om utkastet § 13 annet ledd

Utkastet § 13 annet ledd rammer den som «på annen måte uberettiget foretar handling som er egnet til vesentlig å hindre driften av et datasystem eller et elektronisk kommunikasjonsnett». Bestemmelsen retter seg mot forsettlig misbruk av et datasystem for å oppnå driftshindring. Driftshindringen kan ramme datasystemet eller det elektroniske kommunikasjonsnettet. Det siste vil ofte være en indirekte konsekvens av at det har oppstått driftshindring for datasystemet. I motsetning til handlingen beskrevet i første ledd, skapes ikke driftshindringen av ekstern påvirkning på datasystemet eller det elektroniske kommunikasjonsnettet. Formålet med strafferegelen i utkastet § 13 annet ledd, er særlig å ramme rettsstridig iverksettelse av prosesser som resulterer i at datasystemet eller det elektroniske kommunikasjonsnettet settes ut av funksjon på grunn av kapasitetssvikt, når dette skjer av en bruker som allerede er berettiget til å benytte systemet. Handlingen reiser spørsmål om forholdet mellom utkastet § 8 og utkastet § 13, se nedenfor.

Et eksempel på overtredelse av utkastet § 13 annet ledd er å starte et program som har som formål å sluke datasystemets kapasitet, for eksempel ved kontinuerlig å restarte seg selv (bakterieprogram). Et slikt program vil også anses som et skadelig program og annen befatning med det er straffbar etter utkastet § 11.

### 9.13.4 Forholdet til utkastet § 8

Etter omstendighetene kan tilfeller av ulovlig bruk av datasystem, jf. utkastet § 8, skape så stor belastning på datasystemet eller det elektroniske kommunikasjonsnettet at det har driftshindring til følge. Dersom driftshindringen lå utenfor forsettet rammes handlemåten av utkastet § 8, men driftshindringen kan gjøre lovbruddet grovt og har betydning for straffutmålingen.

Dersom driftshindringen lå innenfor forsettet for den ulovlige bruken av datasystemet, jf. utkastet § 8, oppstår spørsmålet om forholdet til utkastet § 13. Først drøftes forholdet mellom utkastet § 8 og utkastet § 13 første ledd.

Første spørsmål er om fremgangsmåten er slik at den rammes av utkastet § 13 første ledd. Det å utføre et tjenestenektangrep fra sin egen datamaskin rammes ikke av det alternativet i utkastet § 8 som gjelder «datasystem», fordi den uberettigete bruken bare er straffbar dersom datasystemet tilhører en annen. Imidlertid vil handlemåten nødvendigvis representere ulovlig bruk av det elektroniske kommunikasjonsnettet som benyttes til dataoverføringen, og dette vil regulært ikke tilhøre gjerningspersonen. Denne bruken er straffbar etter utkastet § 8, som har et alternativ for misbruk av «elektronisk kommunikasjonsnett» som tilhører en annen. I et slikt tilfelle konsumeres den ulovlige bruken av utkastet § 13 som den strengere bestemmelse. Videre er det klart at dersom en person benytter *en annens datasystem* og utfører et tjenestenektangrep fra dette, er denne bruken straffbar etter utkastet § 8, mens selve driftshindringen rammes av utkastet § 13. Utkastet § 8 vil følgelig iblant kunne anvendes i konkurrens med utkastet § 13 første ledd.

Dersom driftshindringen utføres fra det datasystem som utsettes for driftshindringen, det skjer for eksempel innen datanettverket til en bedrift, oppstår spørsmålet om forholdet mellom utkastet § 8 og utkastet § 13 annet ledd. De subjektive forhold er avgjørende. Dersom forsettet omfatter driftshindringen er utgangspunktet at utkastet § 8 konsumeres av utkastet § 13 som den strengere bestemmelse. Selve installasjonen av det skadelige

programmet, dvs. før det blir satt i gang på datasystemet, kan imidlertid anses som en rettsstridig handling i seg selv, som er straffbar etter utkastet § 8. Ved å anvende utkastet § 8 i realkonkurrens med utkastet § 13 annet ledd får man i tillegg frem dette straffbare elementet ved handlingen.

### 9.13.5 Strafferammer

Den ordinære strafferammen foreslås satt til bøter eller fengsel inntil 6 år. Ved grov overtredelse øker strafferammen til fengsel inntil 10 år. Det vises til begrunnelsen i kapittel 5.6.4.

## 9.14 Utkastet § 14. Masseutsendelse av elektroniske meldinger

Utkastet § 14 lyder:

> «For ulovlig masseutsendelse straffes den som sender elektroniske meldinger som ledd i masseutsendelse til mottakere som ikke har samtykket. Denne bestemmelsen gjelder ikke utsendelse av meldinger i eksisterende kundeforhold, til medlemmer eller lignende med mindre mottakeren har reservert seg mot slike meldinger.
>
> Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.»

Bestemmelsen gjør det straffbart å sende ut spam eller «søppelpost». Det vises til kapittel 3.6 om skadevirkningene av spam, og kapittel 5.6.6 om utvalgets overveielser.

Straffebudet rammer «den som sender elektroniske meldinger som ledd i masseutsendelse til mottakere som ikke har samtykket». Enhver utsendelse er gjort straffbar, jf. «den som sender». Det stilles ikke noe vilkår utover dette, som for eksempel at melding skjer i næringsvirksomhet. Årsaken er at skadevirkningene av spam er de samme uavhengig av omstendighetene rundt sendingen eller formålet med den. Rettsstridsreservasjonen i utkastet § 14 første ledd annet punktum har imidlertid betydning blant annet i næringsvirksomhet, se nedenfor.

Det stilles ikke noen krav til mottaker, for eksempel om at adressaten er en fysisk person. Også spam sendt til bedrifter, forvaltningen, organisasjoner m.v. omfattes av utkastet § 14. Også helt upersonlige meldinger som sendes til adresser av typen post@bedrift.no, rammes. Bestemmelsen dekker følgelig et videre område enn markedsføringslovens forbud mot spam, jf. markedsføringsloven § 2 b, som er begrenset til å gjelde utsendelser «i næringsvirksomhet» til «fysiske personer». På den annen side er utkastet § 14 strengere enn markedsføringsloven § 2 b, ved at den stiller som krav at det er tale om en masseutsendelse (se om begrepet nedenfor). Etter markedsføringsloven § 2 b er det tilstrekkelig med utsending av en melding som oppfyller bestemmelsens vilkår, men i praksis blir den bare anvendt overfor spam, det vil si masseutsendelse. Det foreslås derfor at utkastet § 14 erstatter deler av markedsføringsloven § 2 b.

Utsendelsesforbudet i utkastet § 14 gjelder «elektroniske meldinger» og disse må sendes «som ledd i masseutsendelse». Det er et vilkår at mottakeren «ikke har samtykket» til sendingen.

«Elektroniske meldinger» omfatter elektronisk kommunikasjon som har en slik form at melding kan sendes til et teknisk mottak («innboks») uten at mottakeren behøver å motta meldingen rent fysisk. Dette innebærer en avgrensning mot såkalt forbindelsesorientert kommunikasjon, typisk telefoni, hvor kommunikasjonen forutsetter at mottakeren stiller seg tilgjengelig for å motta samtalen. Markedsføringshenvendelser pr. telefon omfattes følgelig ikke av utkastet § 14, men kan rammes av markedsføringsloven § 2 b, dersom det skjer ved bruk av automatisert oppringningssystem.

Uttrykket «elektroniske meldinger» skal ellers forstås som et teknologinøytralt uttrykk. Det omfatter for eksempel e-post meldinger, meldinger til news, til hjemmesider på internett med interaktive funksjoner, tekst- og multimediameldinger pr. mobiltelefon. Videre omfattes masseutsendelse av telefaksmeldinger.

Den elektroniske meldingen må være sendt «som ledd i masseutsendelse til mottakere som ikke har samtykket». Som det fremgår er «masseutsendelse» den rettslige betegnelse på spam. Straffebudet inneholder ikke noen nærmere spesifikasjon av hva som kjennetegner spamutsendelse bortsett fra at det må være tale om adressater som ikke har samtykket. Dette samtykket må være gitt på forhånd, det vil si før utsendingen skjer. Det er for eksempel ikke tilstrekkelig for å oppfylle samtykkekravet at tittellinjen i meldingen oppfordrer til å gi samtykke (for eksempel «Do you accept this mail?» eller «Do you want to read this offer?»).

Hvorvidt det er tale om en masseutsendelse beror på en totalvurdering. Det ligger i sakens natur at det må være tale om en melding som sendes til mange adressater, men som det fremgår av overveielsene i kapittel 5.6.6, er det ikke hensiktsmessig å tallfeste noe minsteantall. Uttrykket masseutsendelse krever heller ikke at antall adressater kan fastlegges eksakt i en gitt sak, men det må

fremstå som klart at meldingen har gått til flere som ikke har samtykket. Det antas at meldingens innhold i seg selv vil kunne bidra til å kaste lys over denne omstendigheten.

Sendingen må skje samtidig eller innenfor et kort tidsrom, til alle adressatene, ellers blir det tale om en individuell sending som ikke rammes av utkastet § 14. Det må dog ses hen til de nærmere omstendighetene. Dersom det programmet (spamprogrammet) som anvendes for forsendelse er instruert om å sende meldinger med et visst mellomrom, kan det bli ansett som en omgåelse som likevel anses som masseutsendelse, jf. utkastet § 14.

Meldingens innhold er uten betydning, Det typiske er at det gjelder markedsføringshenvendelser av forskjellig art, men også meldinger med ideelt og politisk innhold omfattes. Det antas at spamforbudet ikke er i strid med ytringsfriheten, jf. merknadene i kapittel 5.6.6.

Et annet kjennetegn på en masseutsendelse er om utsendelsen er basert på adresselister som innsamlet i strid med regler i personvernlovgivningen, eventuelt annen straffbar atferd, for eksempel ved overtredelse av utkastet §§ 5, 6 eller 9. Dette er ikke et ubetinget vilkår, men et tungtveiende moment i helhetsvurderingen.

Bestemmelsen rammer den som «sender» meldinger som nevnt. Med «sender» tenkes det på den som kontrollerer utsendelsen av spam, det vil si beslutter, tilrettelegger og iverksetter utsendelsen. I praksis sendes spam ofte ved å misbruke en tredjeparts datasystem for selve den tekniske utsendelsen (se kapittel 3.6). Denne tredjeparten rammes ikke av utkastet § 14, med mindre vedkommende har samtykket til eller på annen måte aktivt tilrettelagt for bruk av datasystemet til masseutsendelse. I så fall kan vedkommende straffes for medvirkning til overtredelse av utkastet § 14, jf. ny straffelov § 15. Regulært vil tredjeperson være uvitende om misbruket, og er selv offer for straffbar handling i forbindelse med spamutsendelsen. Bruken av datasystemet kan etter omstendighetene rammes av utkastet §§ 4 og 8, og eventuelt § 13 dersom de automatiske bekreftelsene fra mottakernes datasystemer utgjør en så stor belastning at det representerer driftshindring.

Masseutsendelse er ikke straffbart dersom det skjer «i eksisterende kundeforhold, til medlemmer eller lignende». Dette gjelder likevel ikke dersom «mottakeren har reservert seg mot slike meldinger». Denne regelen i utkastet § 14 første ledd annet punktum innskrenker området for spamforbudet etter mønster fra markedsføringsloven § 2 b. Årsaken er at spamforbudet ikke bør ramme bruk av elektroniske meldinger i vanlig kundepleie, kontakt med medlemmer i en forening eller annen type organisasjon m.v. Det samme gjelder utsendelse av offentlig informasjon fra forvaltningen til borgerne. I disse tilfellene er ikke utsendelsen rettsstridig selv om forhåndssamtykke ikke er innhentet, jf. § 14 første punktum.

Det avgjørende for rettsstridsreservasjonen er karakteren av den relasjon som foreligger mellom avsender og mottaker, det vil si om det kan karakteriseres som «eksisterende kundeforhold», et medlemskap eller lignende. Det følger uttrykkelig av ordlyden at masseutsendelse ikke rettmessig kan anvendes med sikte på å opprette nye kundeforhold m.v., det er kun tale om masseutsendelse i «eksisterende» relasjoner. Det er ikke en betingelse etter loven at det er tale om relasjoner i næringsvirksomhet. Reservasjonen i første ledd annet punktum omfatter for eksempel også elektronisk kommunikasjon mellom private, for eksempel invitasjoner til større private arrangementer som sendes med e-post.

Av annet punktum siste alternativ fremgår det at dersom masseutsendelse skjer til mottakere i slike eksisterende relasjoner, er utsendelse likevel rettsstridig dersom mottakeren har reservert seg. Den generelle reservasjonen i det sentrale reservasjonsregisteret vil være å anse som en gyldig reservasjon, jf. utkastet § 14. Det samme gjelder reservasjon som er foretatt direkte overfor den annen part.

## 9.15 Utkastet § 15. Identitetstyveri og bruk av uriktig identitet

Utkastet § 15 lyder:

> «For identitetstyveri straffes den som uberettiget bruker uriktig identitet ved elektronisk kommunikasjon. Som uriktig identitet anses identiteten til en annen fysisk eller juridisk person og identitet som ikke tilhører noen.
>
> Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder. »

Det vises til de generelle merknadene i kapittel 5.6.7.

Utkastet § 15 rammer bruk av uriktig identitet ved elektronisk kommunikasjon. Gjerningsbeskrivelsen første ledd første puntum karakteriserer den straffbare handling som identitetstyveri, men bestemmelsen går lenger enn dette siden den også rammer rettsstridig bruk av identitet som ikke til-

hører noen, det vil si rent fiktiv identitet. Det sentrale begrepet er «uriktig identitet» og dette er definert i bestemmelsens første ledd annet punktum som følger: « Som uriktig identitet anses identiteten til en annen fysisk eller juridisk person og identitet som ikke tilhører noen». Uriktig identitet inndeles følgelig i to hovedkategorier, og det er bare bruk av identitet som tilhører en annen («stjålet identitet») som innebærer en krenkelse av den personlige integritet. Men for begge kategoriene gjør hensynet til sikker kommunikasjon seg gjeldende, siden mottakeren kan ha behov for å stole på de identitetsopplysninger som gis.

Første alternativ i definisjonen gjelder identitet som tilhører en annen («stjålet identitet»). Innehaveren av identiteten kan være en fysisk eller juridisk person, for eksempel en bedrift eller en organisasjon. Annet alternativ gjelder identitet som ikke tilhører noen («fiktiv identitet»). En identitet kan være fiktiv selv om den fremstår som et naturlig navn. Avgjørende er at den ikke tilhører noen. Grensetilfelle oppstår dersom identiteten tilhører noen, men gjerningspersonen ikke var klar over det. Subsumsjonsspørsmålet har imidlertid ikke betydning for straffeskylden siden alternativene er likestilte. Bruk av identiteten til en død person eller til en bedrift eller organisasjon som har opphørt å eksistere antas å måtte bedømmes som fiktiv identitet. Det avgjørende er at identiteten ikke tilhører noen på gjerningstidspunktet.

Hvorvidt opplysningen er å anse som «identitet» må avgjøres på grunnlag av en totalvurdering hvor konteksten har stor betydning, Det er med andre ord vesentlig om kommunikasjonen skjer i et miljø eller i en situasjon hvor det er grunn til å forvente at opplysningen er reell. På en del elektroniske tjenester er det vanlig å benytte pseudonymer (se kapittel 5.6.7 om dette begrepet). Når deltagerne ikke kan ha noen forventning om at de øvrige oppgir reell identitet har heller ikke opplysningen noen relevans, og er neppe å anse som en identitet i straffebudets forstand. En annen innfallsvinkel er å si at bruken under enhver omstendighet ikke kan være rettsstridig i et slikt tilfelle (se kapittel 5.3.5). Dette gjelder selv om man har anvendt et navn som viser seg å tilhøre en annen. Men slik bruk kan være rettsstridig etter andre regler, for eksempel etter straffeloven § 390 a.

Således vil heller ikke registrering under uriktig identitet på tjenester beregnet på barn og ungdom uten videre være rettsstridig, jf. utkastet § 15. Tvert imot kan slik opptreden være i samsvar med nettvettregler, og det rammes da ikke av utkastet § 15. Rettsstridsvilkåret skal forstås slik at det støtter andre regler til vern om barn om ungdom som en sårbar brukergruppe, som for eksempel de foreslåtte reglene i straffeloven § 201 annet ledd i forbindelse med tiltak mot «grooming». Mottakeren av opplysningen har heller ikke foranledning til å stole på informasjonen i slike tilfeller. Det vises også her til kapitlet om nettvett (kapittel 5.3.5).

Hvilke opplysninger som kan skape «identitet» kan variere, men navn, adresse, e-postadresser hvor person- eller bedriftsnavn inngår er åpenbart relevante. I tillegg kan domenenavn og innhold (det visuelle uttrykket) på et nettsted være slike opplysninger. Det samme gjelder informasjon som gis i løpet av en samtale på en pratekanal. Det vises til kommentarene i kapittel 5.6.7 om dette.

## 9.16 Utkastet § 16. Kontomisbruk

Utkastet § 16 lyder:

> «For kontomisbruk straffes den som med forsett om vinning uberettiget disponerer over en konto som tilhører en annen, ved å gi opplysninger til et datasystem og derved volder tap eller fare for tap for noen. Med konto menes en adgang til bestemte rettigheter basert på et avtaleforhold, og informasjon om rettighetene er lagret elektronisk.
>
> Med konto menes en adgang til bestemte rettigheter av økonomisk art basert på et avtaleforhold når informasjonen om rettighetene er lagret elektronisk. Det anses ikke som konto dersom informasjonen om rettighetene kun er lagret elektronisk i en fysisk representasjon som kan utnyttes av ihendehaveren.
>
> Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.»

Det vises til merknadene i kapittel 5.8.5.

Straffebudet retter seg mot kontomisbruk. Straffebudet retter seg mot tredjepersons misbruk av en annens konto, jf. «konto som tilhører en annen». Kontoinnehaverens eget misbruk, for eksempel ved forsettlig overbelastning av konto, omfattes ikke av bestemmelsen.

«Konto» er definert i bestemmelsens annet ledd. Det sentrale er at det er tale om rettigheter av økonomisk verdi. Videre er det et vilkår at selve administrasjonen av rettigheten skjer av en annen enn kontoinnehaveren selv. Et typisk eksempel på kontoforhold som omfattes av definisjonen er bankkonti. Det er uten betydning om beløpet på konto er et tilgodehavende eller en gjeld (kreditt) for kontohaver. Poenget er bevegelsene på konto registreres av den som administrerer kontoen.

Dette kan være en bank, et kredittforetak, en oppgjørsagent m.v. Også andre avtaleforhold kan representere konti i bestemmelsens forstand, for eksempel en konto med bonuspoeng hos et flyselskap eller et abonnement i et teleselskap.

Kontobegrepet kan – og vil ofte være – representert fysisk, for eksempel ved et bank- eller kredittkort, men dette er ikke noe rettslig relevant vilkår.

Kontobegrepet i utkastet § 16 avgrenses mot elektroniske ihendehaverbevis, jf. bestemmelsens annet ledd annet punktum. Med dette menes kort, armbånd m.v. som er utstyr med elektronisk brikke som gir rett til å disponere over et visst beløp. Slike betalingsløsninger er vanlige, for eksempel i svømmehaller eller på festivaler. Også elektroniske telefonkort pålydende et gitt beløp eller et begrenset antall tellerskritt faller i denne gruppen. Dersom slike ihendehaverbevis urettmessig borttas eller tilegnes, står man overfor regulært tyveri eller underslag. Bruken av beløpet er å anse som et moment i straffutmålingen.

Straffebudet rammer det å uberettiget disponere konto som nevnt. Formuleringen setter ikke noen begrensninger for hva slags type handlinger det er tale om, annet enn at det ikke omfatter disposisjoner foretatt av kontoinnehaver selv (eller noen som opptrer på vedkommendes vegne).

Eksempler på uberettiget disponering av konto kan være å anvende et stjålet kort eller et kort som er ulovlig kopiert (skimming), på en automat for uttak av kontanter eller varer. Et tilfelle som nevnt i Rt. 1997 side 1771 hvor det ble foretatt uttak av bensin og varer med bruk av kort som var ulovlig kopiert, skal derfor ikke lenger bedømmes som tyveri, men som kontomisbruk, jf. utkastet 16. Det samme gjelder avgivelse av opplysning om en annens kredittkortnummer og sikkerhetskode ved bestillinger på internett.

Som det fremgår har karakteren av vinning ikke betydning for subsumsjonen. Dette er en endring i forhold til gjeldende rett. Dersom vilkårene for øvrig er oppfylt etter utkastet § 16, skal dette under enhver omstendighet bedømmes som kontomisbruk.

Det er et vilkår at det voldes tap eller fare for tap for noen. Dette tilsvarer formuleringen i databedrageribestemmelsen i straffeloven § 270 første ledd nr. 2 og skal forstås likedan. Om uttrykket «noen» kan det bemerkes at det vil kunne være både medkontrahent, kontoutsteder og kontoinnehaver.

## 9.17 Utkastet § 17. Grovt uaktsomt datalovbrudd

Utkastet § 17 lyder:

> «Er bestemmelser i §§ 7, 9, 10, 12 annet ledd eller 13 i dette kapitlet overtrådt uten forsett, er overtredelsen likevel straffbar hvis gjerningspersonen har opptrådt grovt uaktsomt. »

Det vises til de generelle merknadene under kapittel 6.1.

Skyldkravet etter datakrimkapitlet er som hovedregel forsett, men etter denne bestemmelse er §§ 7, 9, 10, 12 annet ledd og 13 også straffbar dersom gjerningspersonen opptrådte grovt uaktsomt. Utvalget har kommet til at disse bestemmelser bør være straffbare også ved grov uaktsomhet ut fra en vurdering av hvilke overtredelser som praktisk kan begås ved uaktsomhet sett i forhold til skadepotensialet ved overtredelse. Også bevisbyrdereglene taler for at visse grovt uaktsomme overtredelser er straffbare, idet forsett i en del tilfeller er vanskelig å bevise (for å ramme «skjult forsett»).

Utvalget har vurdert om også simpel uaktsomhet bør være straffbar for enkelte av bestemmelsene, men finner at det bør kreves grov uaktsomhet. Om dette vises det til kapittel 6.1.

Når det gjelder hvilke overtredelser som etter utkastet også er straffbare ved grov uaktsomhet, bemerker utvalget at for en del av bestemmelsene er det vanskelig å tenke seg at en handling kan begås ved uaktsomhet. Dette gjelder for eksempel utkastet § 2 (elektronisk kartlegging), § 3 (ulovlig anbringelse av utstyr), § 14 (masseutsendelse av elektroniske meldinger) og § 16 (kontomisbruk). Kravet til uberettiget vil også utelukke noen av handlingene, for eksempel § 15 (identitetstyveri og bruk av uriktig identitet).

Når det gjelder § 4 (ulovlig tilgang til datasystem) bemerker utvalget at normaltilfellet ved overtredelse av denne bestemmelse er at det foretas en aktiv handling fra gjerningspersonens side. Etter utvalgets syn vil det normalt ikke foreligge særlige problemer med å bevise forsettet dersom hendelsesforløpet kan bevises. Det kan imidlertid tenkes tilfeller av ulovlig tilgang som reelt skyldes uaktsomhet fra gjerningspersonens side. Vedkommende vil for eksempel kjøre en exploit mot sitt eget system for å teste sikkerheten, men skriver inn feil IP-addresse og skaffer seg dermed ulovlig tilgang på et annet system. Det kan også tenkes andre eksempler som begås ved uaktsomhet. Hvorvidt slik uaktsomhet anses som grov vil variere fra tilfelle til tilfelle. Utvalget finner imidlertid grunn til å spørre om skaden som oppstår ved ulov-

lig tilgang begått ved uaktsomhet er tilstrekkelig stor til å begrunne å belegge dette med straff. I eksemplet som er nevnt over vil gjerningspersonen raskt oppdage at han er inne på en annens datasystem. Eventuell videre bruk av systemet vil da bli forsettlig ulovlig bruk (utkastet § 8), data/informasjonstyveri (utkastet §§ 5 og 6) eller datamodifikasjon (§ 7). Skaden som oppstår ved selve tilgangen er at systemsikkerheten er brutt. Utvalget er av den oppfatning at denne skaden ikke er så betydelig at den kan begrunne at grov uaktsom overtredelse av § 4 bør være straffbar.

For utkastet § 5 (informasjonstyveri) viser utvalget til at gjerningen som utføres her er at man tilegner seg informasjon som man ikke skulle ha tilgang til. Det kan med andre ord være nok å lese fra skjermen over skulderen til andre, eller på annen måte uberettiget få kjennskap til datalagret informasjon. Utvalget finner at det er åpenbart at dette er et forhold som lett kan oppstå ved uaktsomhet, og spørsmålet blir da hvilken aktsomhet man har plikt til å utvise når det gjelder å få informasjon som man ikke skulle hatt tilgang til. Utvalget mener at det vil føre for langt å gjøre også grovt uaktsomme handlinger etter denne bestemmelsen straffbare.

Heller ikke utkastet § 6 (datatyveri) finner utvalget bør gjøres straffbart ved grov uaktsomhet. Et datatyveri skjer riktignok ikke så lett som et informasjonstyveri, men krever i større grad en aktiv handling fra gjerningspersonens side. For eksempel kan det tenkes at en ansatt som slutter i en bedrift kopierer med seg private filer, men også får med seg bedriftens filer, uten at det var bevisst. Utvalget er likevel kommet til at også for § 6 bør det kreves forsett.

I forhold til utkastet § 7 (datamodifikasjon) finner imidlertid utvalget at dette er handlinger som bør være straffbare også dersom de begås ved grov uaktsomhet. Endring eller sletting av data er handlinger som meget lett kan skje ved uaktsomhet, og dette kan potensielt få meget store konsekvenser. Det er for eksempel fullt mulig å slette alle data som er lagret på et datasystem på en slik måte at de ikke kan rekonstrueres. Dette vil for eksempel skje hvis en dataetterforsker ved speilkopiering foretar kopieringen i feil retning, slik at originaldisken blir overskrevet. En slik feil må ofte karakteriseres som grovt uaktsom i og med at dette er det aller viktigste dataetterforskeren skal passe på. De potensielt store skadefølgene er for utvalget avgjørende for at grovt uaktsom datamodifikasjon bør være straffbar.

Uberettiget bruk av datasystem etter utkastet § 8 er også en aktiv handling. Utvalget kan imidlertid vanskelig se at uaktsomhet vil ha noen praktisk anvendelse i forhold til denne bestemmelsen. Det måtte eventuelt være uaktsomhet som går ut på hvem som er den egentlige eier av systemet.

Utkastet § 9 (etterfølgende befatning av ulovlig tilegnet data og databasert informasjon) er imidlertid en bestemmelse hvor uaktsomhet er meget aktuelt. Man kan for eksempel tenke seg at informasjonen blir publisert på et websted ved uaktsomhet, og at dette får store konsekvenser fordi den da blir kjent for allmennheten. Dersom handlingen kan karakteriseres som grovt uaktsom er det etter utvalgets syn klart at det bør gjøres straffbart på grunn av skadepotensialet.

Det samme gjelder for utkastet § 10 (ulovlig befatning med tilgangsdata). Et eksempel kan være en systemadministrator som sender ut passordene til alle brukerne i klartekst til et newsforum. Dette er noe alle systemadministratorer vet at de ikke skal gjøre, og vil lett karakteriseres som grovt uaktsomt. Skadepotensialet ved en slik handling er så stort at utvalget finner at også grovt uaktsomme handlinger bør være straffbare.

For handlinger som dekkes av utkastet § 11 (befatning med skadelig dataprogram og utstyr) bør det etter utvalgets oppfatning kreves forsett, mens når det gjelder utkastet § 12 annet ledd (befatning med selvspredende dataprogram) og utkastet § 13 (driftshindring) bør det etter utvalgets syn være tilstrekkelig med grov uaktsomhet. Det vises til at overtredelser etter § 12 annet ledd har meget stort skadepotensiale. Er man først klar over at man har selvspredende dataprogram mellom hendene, må det kreves at man innretter seg slik at det ikke uforvarende startes opp. Grov uaktsomhet i så henseende bør derfor være straffbart. Drifthindring etter § 13 skjer normalt ved forsettlige handlinger, men kan også oppstå ved uaktsomhet som følge av at den som kjører et dataprogram ikke innser at følgen av dataprogrammet er at det oppstår en driftshindring for noen. Dette vil etter omstendighetene kunne bedømmes som grovt uaktsomt, og bør etter utvalgets syn rammes.

I kravet om grov uaktsomhet ligger at handlingen er svært klanderverdig og at det er grunnlag for sterk bebreidelse, jf. ny straffelov § 23 annet ledd, og Ot.prp. nr. 90 (2003-2004) side 427. Det vises også til Rt. 1970 side 1235 hvor det fremgår at for grov uaktsomhet må det foreligge en kvalifisert klanderverdig opptreden som foranlediger sterke bebreidelser for mangel på aktsomhet.

Utvalget har vurdert om det bør gis egne strafferammer for de grovt uaktsomme handlinger, men er kommet til at man ikke vil foreslå det. Det vises til begrunnelsen gitt under kapittel 6.1.

## 9.18 Utkastet § 18. Grovt datalovbrudd

Utkastet § 18 lyder:

> «Ved avgjørelsen av om et lovbrudd etter dette kapitlet skal anses som grovt, legges det særlig vekt på den skade som er voldt eller kunne ha vært voldt, om lovbruddet er begått ved å bryte en beskyttelse og om gjerningspersonen har hatt eller kunne ha hatt vinning og størrelsen av denne.»

Det vises til de generelle merknadene under kapittel 6.2.

Oppregningen i bestemmelsen over av hva om gjør en handling til et grovt datalovbrudd, er ikke er uttømmende. Dette fremgår ved uttrykket «legges det *særlig* vekt på». Det vil avhenge av en helhetsvurdering av om handlingen anses som en grov overtredelse. Selv om ett eller flere av alternativene i § 18 er til stede, innebærer ikke det nødvendigvis at handlingen anses som en grov overtredelse. På samme måte kan handlingen også anses som grov, selv om ingen av de nevnte alternativene foreligger, dersom andre forhold tilsier det. De alternativene som er nevnt i § 18 er imidlertid etter utvalgets oppfatning momenter som ofte vil bringe forholdet inn i karakteristikken grovt datalovbrudd.

Når det gjelder alternativene, er det særlig den voldte skade som innebærer at forholdet bør anses som grovt. Utvalget finner imidlertid at det ikke bare er den konkrete skaden som bør tillegges vekt, men også skadepotensialet. Det vises til at det i en del tilfeller vil være tilfeldig om skade faktisk blir voldt. For eksempel kan sikkerhetstiltak hos den som blir angrepet begrense skaden, uten at dette bør ha betydning for hvordan gjerningspersonens forhold bedømmes. Videre er det i mange tilfeller vanskelig å skaffe seg et sikkert overslag over den faktiske skaden som er voldt.

I begrepet «skade» ligger naturligvis den økonomiske skade som lar seg beregne. Utvalget legger imidlertid en bredere forståelse av begrepet til grunn, idet man også mener at uleilighet, forsinkelse og problemer hos andre må anses som skade, selv om det ikke lar seg beregne noe økonomisk tap. Hvor stor skade som må kreves for å bedømme forholdet som grovt, må avgjøres konkret. Her vil man for økonomisk skade måtte se hen til hvor grensene for grove vinningsforbrytelser går, for tiden ved ca. kr 100 000. Når det gjelder annen skade enn den økonomiske, vil man måtte se hen til hvor mange som er rammet av handlingen og omfanget mer generelt.

Det neste alternativet som skal vektlegges ved vurderingen av om forholdet anses som grovt, er om det er begått ved å bryte en beskyttelse. Der den som er rammet har forsøkt å beskytte seg ved for eksempel tilgangskoder eller kryptering, eller på andre måter, er dette et moment som etter utvalgets syn taler for å bedømme forholdet som grovt.

Videre finner utvalget at gjerningspersonens vinning og den eventuelle størrelsen av denne også bør tillegges vekt ved vurderingen av om forholdet skal anses som grovt. Opplysninger utvalget har fått under sitt arbeid, tyder på at det på datakrimområdet har skjedd en dreining fra å være forhold begått ut fra utforskertrang, nysgjerrighet og for å oppnå anerkjennelse fra andre i miljøet, til å bli mer vinningsstyrt kriminalitet. Dette gir forholdene, etter utvalgets oppfatning, en annen og mer alvorlig karakter, og bør tillegges vekt i vurderingen av om forholdet anses som grovt eller ikke.

## 9.19 Utkastet § 19. Lite datalovbrudd

Utkastet § 19 lyder:

> «Ved avgjørelsen av om et lovbrudd etter dette kapitlet skal anses som lite, legges det særlig vekt på om skadepotensialet er lite og om gjerningspersonen ikke har eller kunne ha hatt vinning.»

Det vises til de generelle merknadene under punkt 6.2.

Oppregningen i bestemmelsen over av hva som gjør en handling til et lite datalovbrudd, er ikke er uttømmende. Dette fremgår ved uttrykket «legges det *særlig* vekt på«. Det vil avhenge av en helhetsvurdering om handlingen anses som en liten overtredelse. Selv om ett eller begge av alternativene i utkastet § 19 er til stede, innebærer ikke det nødvendigvis at handlingen anses om en liten overtredelse. Videre kan handlingen også anses som liten, selv om ingen av de nevnte alternativene foreligger, dersom andre forhold tilsier det. De alternativene som er nevnt i utkastet § 19 er imidlertid etter utvalgets oppfatning momenter som ofte vil bringe forholdet inn i karakteristikken lite datalovbrudd.

Utvalget har kommet til at det er særlig lite skadepotensiale og manglende vinningsmuligheter som bør være avgjørende for om forholdet skal anses som et lite datalovbrudd. Med skadepotensiale mener utvalget både økonomisk og ikke-økonomisk skade som beskrevet i merknaden til utkastet § 18. Ved vurderingen av om forholdet anses som lite, finner utvalget at det ikke er den voldte skade, men potensialet for skade som bør være avgjørende, idet tilfeldigheter kan føre til at den faktiske skaden blir liten selv om potensialet var stort.

Dette bør ikke komme gjerningspersonen til gode i karakteristikken av forholdet.

Også manglende faktisk vinning eller vinningsmuligheter bør vektlegges i vurderingen.

Utvalget har vurdert om gjerningspersonens alder, erfaring og hensikt bør tas med i oppregningen av momenter som tilsier at forholdet anses som et lite datalovbrudd. Utvalget har imidlertid kommet til at dette ikke bør tas med. Det vises til at selv om gjerningspersonen er ung, og kanskje har liten erfaring, kan vedkommende begå handlinger som etter utkastet § 18 skal vurderes som grove datalovbrudd. Ung alder, liten erfaring og begrenset forståelse av skadepotensialet, vil etter rettspraksis ha betydning for den konkrete straffutmåling innenfor den aktuelle strafferamme, og bør da etter utvalgets oppfatning ikke ha betydning for om forholdet skal anses som grovt, vanlig eller lite.

# Kapittel 10
# Økonomiske og administrative konsekvenser

Forslagene til endringer i straffeloven viderefører dagens straffelov på noen områder, presiserer området for det straffbare på noen punkter og utvider området på andre områder. Lovforslagene har til formål å bekjempe datakriminalitet mer effektivt. Det er lagt vekt på at lovforslaget skal representere et godt verktøy for alle som arbeider med å bekjempe datakriminalitet, herunder påtalemyndigheten og domstolene. Dette kan føre til flere pådømmelser og lengre utmålt straff. Bestemmelsene vil derfor gi økt belastning på strafferettsapparatet og føre til behov for flere fengselsplasser.

Når det gjelder nykriminalisering foreslår utvalget i utkastet § 2 en ny bestemmelse som skal gi mulighet til å straffe elektronisk kartlegging av datasystemer. Bestemmelsen er ment å ramme kartlegging av sårbarheter i andres datasystemer. Slik kartlegging er ofte første skritt på veien for å begå datakriminalitet. Avhengig av påtalemyndighetens prioriteringer kan forslaget komme til å øke påtalemyndighetens arbeidsbyrde dersom det blir vedtatt. Bruken av en bestemmelse som rammer datakriminalitet på et tidlig tidspunkt gir imidlertid politiet mulighet til å gripe inn tidligere, og kan derfor bli et viktig verktøy i arbeidet mot datakriminalitet. Dette kan igjen gi økonomiske besparelser for både politiet og for samfunnet på sikt. Utvalget finner det derfor vanskelig å forutsi hvilke konkrete økonomiske og administrative konsekvenser forslaget totalt sett kan få.

Utvalget foreslår videre i utkastet § 3 en ny bestemmelse om ulovlig anbringelse av utstyr. Bestemmelsen er ment å straffbelegge rettsstridig anbringelse av utstyr på eller i tilknytning til et datasystem eller et elektronisk kommunikasjonsnett. Slikt utstyr anbringes ofte som forberedende ledd i datakriminalitet eller annen kriminalitet, for eksempel et videokamera som plasseres over en minibank for å skaffe tilgang til tilgangskoder eller installering av en nettverkssniffer for å avlytte data som overføres på det elektroniske kommunikasjonsnettet. Avhengig av politiets og påtalemyndighetens prioriteringer kan forslaget føre til økte økonomiske og administrative konsekvenser for myndighetene. På den annen side kan bestemmelsen på sikt også bidra til mindre kriminell aktivitet og dermed føre til økte besparelser både for myndighetene og for private.

Utvalget foreslår i utkastet § 4 et vern mot ulovlig tilgang til datasystem. Bestemmelsen er ment å bidra til å sikre datasystems pålitelighet gjennom å straffebelegge ulovlig tilgang til et datasystem. Bestemmelsen antas å kunne øke påtalemyndighetens arbeidsbyrde. Utvalget finner det imidlertid vanskelig å anslå noe om de økonomiske og administrative konsekvensene dette kan få for politi og påtalemyndighet. Derimot kan det fastslås at bestemmelsen ikke inneholder noe krav om at datasystemet må være beskyttet. Det forutsettes således ingen kostnadskrevende sikringstiltak fra bruker for at datasystemet skal være vernet av bestemmelsen. Forslaget antas derfor ikke å få noen økonomiske og administrative konsekvenser for brukerne.

Utkastet § 5 er en ny bestemmelse om informasjonstyveri og utkastet § 6 er en ny bestemmelse om datatyveri. Hensynet bak bestemmelsene er å gi et generelt strafferettslig vern mot rettsstridig tilegnelse av data og databasert informasjon. Selv om data og databasert informasjon ikke har et selvstendig strafferettslig vern etter gjeldende rett, er det imidlertid flere straffebud som rammer handlinger som reelt sett innebærer en slik tilegnelse. Utvalget mener derfor at bestemmelsene i større grad vil bidra til å klargjøre rettstilstanden enn til reelt sett å utvide straffeområdet. Det er derfor ikke grunn til å anta at de økonomiske og administrative konsekvensene vil bli store ved en innføring av bestemmelsene.

Utvalget foreslår å innta en ny bestemmelse i utkastet § 15 om identitetstyveri som rammer rettsstridig bruk av uriktig identitet. Et slikt straffebud vil gjøre det lettere å verne individer mot å få sin identitet misbrukt og vil på den måten kunne spare enkeltindivider mot økonomiske tap. I tillegg vil samfunnet kunne få en gevinst ved at tilliten til elektronisk kommunikasjon fremmes. Forslaget inneholder en viss nykriminalisering, og uvalget antar derfor at forslaget kan få økonomiske og administrative konsekvenser for justissektoren dersom det blir vedtatt.

Et mindretall i utvalget foreslår at det tas inn en bestemmelse § 76 b om filtrering av steder på internett. Her foreslås det at domstolen skal kunne pålegge tjenesteyter å blokkere tilgang til bestemte steder på internett med ulovlig innhold. Dette er ment som et redskap til å få blokkert internettsider med ulovlig innhold, og vil derfor kunne være et viktig arbeidsredskap for justissektoren. Det vil imidlertid ha sin pris i forhold til tjenestetilbydere som må sikre gjennomføring av slike vedtak. Krav som stilles til mellomliggende aktører, som for eksempel tjenestetilbydere vil kunne føre til dyrere tjenester for publikum. Utvalget antar at dersom mindretallets syn følges og bestemmelsen blir vedtatt, så vil den kunne få økonomiske og administrative konsekvenser både for justissektoren og for private aktører.

Utvalget foreslår å utvide og presisere straffeområdet for enkelte handlinger som i dag delvis er dekket i andre straffebestemmelser i straffeloven og i spesiallovgivningen. Dette gjelder utkastet § 9 om etterfølgende befatning med ulovlig tilegnet data og databasert informasjon, utkastet § 10 om befatning med tilgangsdata, § 11 om befatning med skadelig dataprogram og utstyr og utkastet § 14 om masseutsendelse av elektroniske meldinger.

Utkastet §§ 10 og § 11 kriminaliserer uberettiget befatning med tilgangsdata, skadelig dataprogram og utstyr. Begrunnelsen er blant annet at slike handlinger øker faren for at andre krenkelser begås. Forslag til § 10 innebærer en viss nykriminalisering, da den rammer flere befatningsformer enn bare spredning av tilgangsdata (jf. straffeloven § 145 b). I lys av straffeloven § 262 og åndsverkloven § 53a og § 53c, innebærer § 10 imidlertid bare en mindre nykriminalisering som neppe vil få store økonomiske og administrative konsekvenser. Utkastet § 11 medfører blant annet nykriminalisering for befatning med skadelig dataprogram og utstyr i den grad dette ikke allerede dekkes av straffeloven § 262 første ledd og åndsverkloven § 53a annet ledd og § 53c. De økonomiske og administrative følger innføringen av en slik bestemmelse i praksis vil få, anses å være relativt små.

Utkastet § 14 vil gjøre det straffbart å sende elektroniske meldinger som ledd i masseutsendelse til mottaker som ikke har samtykket (spam). Bestemmelsen går noe videre enn dagens markedsføringslov § 2 b som gjelder spam som sendes i næringsvirksomhet til fysiske personer, og vil dermed kunne ha en bredere anvendelse enn dagens regelverk. Avhengig av påtalemyndighetens prioriteringer vil denne bestemmelsen derfor kunne føre til noe mer ressursbruk for justismyndighetene. I den grad bestemmelsen virker etter sin hensikt, vil den imidlertid sammen med andre virkemidler (tekniske løsninger, bevisstgjøring, selvregulering og internasjonalt samarbeid) kunne føre til store besparelser for brukere av e-post og andre elektroniske kommunikasjonstjenester både i form av mindre behov for kostbare spamfiltere, mindre tidsbruk på uønskede meldinger og bedre kvalitet i de elektroniske kommunikasjonsnettene. I tillegg vil det på sikt kunne få en virkning i form av mindre datakriminalitet, med de økonomiske og administrative virkninger dette vil få.

Utvalget foreslår i tillegg en rekke andre bestemmelser mot datakriminalitet. Lovforslagene er utarbeidet med sikte på å effektivisere bekjempelse av datakriminalitet, noe som også kan få en viss preventiv virkning. Dersom lovforslaget kan bidra til mindre datakriminalitet, enten ved å bremse utviklingen eller ved å redusere dagens nivå, antar utvalget at lovforslaget sett under ett vil kunne føre til samfunnsmessige besparelser. Datakriminalitet påfører både offentlig og privat sektor store utgifter. Selv om enkelte av forslagene vil kunne føre til større ressursbehov for politi, påtalemyndighet, domstolen og kriminalomsorgen, mener utvalget at forslagene på sikt vil kunne bidra til å redusere omfanget av datakriminalitet, med de kostnadene denne kriminalitetsformen fører med seg. Hvilke konkrete økonomiske besparelser lovforslagene kan få for samfunnet dersom det blir vedtatt, er likevel ikke mulig å fastslå.

Vi har i de senere år sett en sterk økning av datakriminalitet. Det er ingen grunn til å vente at dette vil endre seg, uavhengig av lovforslaget. Utvalget finner grunn til å understreke at inngrep for å motvirke datakriminalitet krever økt kompetanse og ressurser både i politiet og i domstolene. Dersom utvalgets forslag blir vedtatt, bør det følges opp med kompetanseoppbygging og ressurstilførsel. I denne sammenheng kan det både hos politiet og hos domstolene være nødvendig å kjøpe inn konsulenttjenester fra sakkyndige. I særlig grad gjelder dette så lenge fagområdet er nytt og ukjent for aktørene. Uten tilgang til tilstrekkelig kompetanse og ressurser vil straffebudene bli vanskelig å følge opp.

# Kapittel 11
# Lovforslag

## 11.1 Nytt kapittel om datakriminalitet

Kapittel X – Vern av data, databasert informasjon og datasystemer

**§ 1** *Definisjoner*
Med følgende uttrykk menes i dette kapitlet:
a) Datasystem: Enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogram.
b) Dataprogram: Data i form av en sekvens instruksjoner som kan utføres i et datasystem, herunder kildekode.
c) Data: Enhver representasjon av informasjon som lagres eller behandles av et datasystem eller som overføres i elektronisk kommunikasjonsnett. I tillegg omfattes enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk utstyr.
d) Databasert informasjon: Meningsinnholdet i data.
e) Elektronisk kommunikasjonsnett: System for elektronisk kommunikasjon der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår.

**§ 2** *Elektronisk kartlegging av datasystem*
For elektronisk kartlegging av datasystem straffes den som over et elektronisk kommunikasjonsnett uberettiget registrerer egenskaper på et datasystem for å kartlegge sårbarheter.

Straffen er bøter eller fengsel inntil 6 måneder. For grov overtredelse er straffen bøter eller fengsel inntil 1 år.

**§ 3** *Ulovlig anbringelse av utstyr m.v*
For ulovlig anbringelse av utstyr straffes den som uberettiget anbringer utstyr på eller i tilknytning til et datasystem eller elektronisk kommunikasjonsnett, for å
a) begå informasjons- eller datatyveri, jf. §§ 5 og 6, eller
b) tilegne seg tilgangsdata som nevnt i § 10.

Det samme gjelder den som installerer dataprogram på et datasystem for å begå handlinger som nevnt.

Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

**§ 4** *Ulovlig tilgang til datasystem*
For ulovlig tilgang straffes den som uberettiget skaffer seg tilgang til hele eller del av et datasystem.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 5** *Informasjonstyveri*
For informasjonstyveri straffes den som uberettiget tilegner seg
a) databasert informasjon, eller
b) utskrift av databasert informasjon.

Straff etter første ledd bokstav b kommer ikke til anvendelse ved handling som går inn under § 257 (tyveribestemmelsen).

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 6** *Datatyveri*
For datatyveri straffes den som uberettiget kopierer, overfører eller på annen måte tilegner seg data.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 7** *Datamodifikasjon*
For datamodifikasjon straffes den som uberettiget endrer, ødelegger, sletter eller skjuler andres data.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 8** *Uberettiget bruk av datasystem m.v.*

For uberettiget bruk straffes den som uberettiget benytter andres datasystem eller elektroniske kommunikasjonsnett. Bruk av andres tilgangspunkt til internett i usikret trådløst elektronisk kommunikasjonsnett anses ikke som uberettiget.

Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

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

For etterfølgende befatning med data og databasert informasjon straffes den som uberettiget benytter, avhender eller tilgjengeliggjør data eller databasert informasjon som er utbytte av en handling som er straffbar etter dette kapitlet.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 10** *Ulovlig befatning med tilgangsdata*

For ulovlig befatning med tilgangsdata straffes den som uberettiget anskaffer, innfører, fremstiller, besitter, markedsfører eller tilgjengeliggjør for andre passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem.

Straffen er bøter eller fengsel i 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

**§ 11** *Skadelig dataprogram og utstyr*

For ulovlig befatning med skadelig dataprogram straffes den som uberettiget anskaffer, fremstiller, modifiserer, besitter, markedsfører eller tilgjengeliggjør dataprogram som er særlig egnet til å begå handlinger som er straffbare etter §§ 4-8, 10 eller 13-14 i dette kapitlet. Liknende befatning med utstyr som er særlig egnet til tilsvarende formål straffes på samme måte.

Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

**§ 12** *Selvspredende dataprogram*

For ulovlig befatning med selvspredende dataprogram straffes den som uberettiget fremstiller, modifiserer, anskaffer eller tilgjengeliggjør selvspredende dataprogram.

For ulovlig befatning med selvspredende dataprogram straffes også den som initierer spredning av slikt program.

Med selvspredende dataprogram menes dataprogram som kan videredistribuere seg til andre datasystemer og installeres automatisk eller ved at noen foretar eller godkjenner installasjonen uvitende om dataprogrammets egenskaper.

Straffen er bøter eller fengsel inntil 1 år. Inneholder det selvspredende dataprogrammet også andre skadelige egenskaper, er straffen bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år.

**§ 13** *Driftshindring*

For driftshindring straffes den som uberettiget overfører data under slike omstendigheter at overføringen vesentlig hindrer eller er egnet til vesentlig å hindre driften av et datasystem eller elektronisk kommunikasjonsnett. Det samme gjelder den som initierer dataoverføring som nevnt.

For driftshindring straffes også den som på annen måte uberettiget foretar handling som er egnet til vesentlig å hindre driften av et datasystem eller elektronisk kommunikasjonsnett.

Straffen er bøter eller fengsel inntil 6 år. For grov overtredelse er straffen fengsel inntil 10 år. For liten overtredelse er straffen bøter eller fengsel inntil 1 år.

**§ 14** *Masseutsendelse av elektroniske meldinger*

For ulovlig masseutsendelse straffes den som sender elektroniske meldinger som ledd i masseutsendelse til mottakere som ikke har samtykket. Denne bestemmelsen gjelder ikke utsendelse av meldinger i eksisterende kundeforhold, til medlemmer eller lignende, med mindre mottakeren har reservert seg mot slike meldinger.

Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

**§ 15** *Identitetstyveri og bruk av uriktig identitet*

For identitetstyveri straffes den som uberettiget bruker uriktig identitet ved elektronisk kommunikasjon. Som uriktig identitet anses identiteten til

en annen fysisk eller juridisk person og identitet som ikke tilhører noen.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 16** *Kontomisbruk*

For kontomisbruk straffes den som med forsett om vinning uberettiget disponerer over en konto som tilhører en annen, ved å gi opplysninger til et datasystem og derved volder tap eller fare for tap for noen.

Med konto menes en adgang til bestemte rettigheter av økonomisk art basert på et avtaleforhold når informasjonen om rettighetene er lagret elektronisk. Det anses ikke som konto dersom informasjonen om rettighetene kun er lagret elektronisk i en fysisk representasjon som kan utnyttes av ihendehaveren.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder.

**§ 17** *Grovt uaktsomt datalovbrudd*

Er bestemmelser i §§ 7, 9, 10, 12 annet ledd eller 13 i dette kapitlet overtrådt uten forsett, er overtredelsen likevel straffbar hvis gjerningspersonen har opptrådt grovt uaktsomt.

**§ 18** *Grovt datalovbrudd*

Ved avgjørelsen av om et lovbrudd etter dette kapitlet skal anses som grovt, legges det særlig vekt på den skade som er voldt eller kunne ha vært voldt, om lovbruddet er begått ved å bryte en beskyttelse og om gjerningspersonen har hatt eller kunne ha hatt vinning og størrelsen av denne.

**§ 19** *Lite datalovbrudd*

Ved avgjørelsen av om et lovbrudd etter dette kapitlet skal anses som lite, legges det særlig vekt på om skadepotensialet er lite og om gjerningspersonen ikke har eller kunne ha hatt vinning.

## 11.2 Endringer i andre paragrafer i ny straffelov

**Kapittel 1: Straffelovgivningens virkeområde**
§ 7 skal lyde slik:

**§ 7** *Handling som anses foretatt på flere steder*

Når straffbarheten av en handling avhenger eller påvirkes av en inntrådt eller tilsiktet virkning, anses handlingen foretatt også der virkningen er inntrådt eller tilsiktet fremkalt. *Er et datasystem eller elektronisk kommunikasjonsnett i Norge rammet eller forsøkt rammet av en handling som er straffbar etter kapitlet om «Vern av data, databasert informasjon og datasystemer», anses virkningen inntrådt i Norge.*

**Kapittel 13: Inndragning**
Straffeloven § 69 annet ledd skal lyde slik:

Som ting regnes også rettigheter, fordringer og elektronisk lagret informasjon*, herunder dataprogrammer.*

Straffeloven § 76 annet ledd skal lyde slik:

Ved inndragning av informasjonsbærer skal det angis hvilke deler av innholdet som begrunner inndragning. Den som må tåle inndragningen, kan mot å dekke utgiftene kreve informasjonsbæreren tilbakelevert etter at det ulovlige innholdet er fjernet. *Gjelder inndragningen data, kan påtalemyndigheten likevel mot at den som må tåle inndragningen dekker utgiftene, i stedet for å tilbakelevere informasjonsbæreren, gi vedkommende en kopi av de data som fantes på informasjonsbæreren og som ikke omfattes av inndragningen.*

Som ny § 76a foreslås:

*§ 76a Særregler for inndragning av konto på datasystem*

*Ved inndragning av en konto på et datasystem kan tjenesteyteren pålegges å stenge domfeltes tilgang til datasystemet og å slette innhold som tilhører domfelte.*

*Inndragning etter første ledd foretas overfor rettighetshaveren til kontoen. Er vedkommende ukjent eller ikke har kjent oppholdssted i Norge, foretas inndragning overfor tjenesteyteren eller besitter av datasystemet såfremt det finnes rimelig av hensyn til rettighetshaveren til kontoen. Inndragning kan foretas overfor andre enn rettighetshaveren til kontoen selv om vedkommende var i god tro. Rettighetshaveren til kontoen skal så vidt mulig gis varsel om saken. Er verken rettighetshaveren til kontoen eller tjenesteyteren kjent eller har oppholdssted i Norge, kan tingretten beslutte inndragning på de vilkår som er nevnt i annet punktum uten at noen er gjort til saksøkt.*

Mindretallsforslag til ny § 76b:

*§ 76b Filtrering av steder på internett*
*Tjenesteyter kan pålegges å blokkere tilgangen til bestemte steder på internett for sine brukere dersom innholdet ville kunne medføre straffansvar i Norge. § 69 tredje ledd, § 71 tredje ledd og § 76a gjelder tilsvarende. De øvrige regler om inndragning gjelder tilsvarende så langt de passer.*

## 11.3 Til øvrige deler av ny straffelov

**Til kapitlet om Vern om den offentlige ro og orden**
Utvalget foreslår ikke at det gis lovbestemmelser for å innarbeide artikkel 6 i tilleggsprotokoll av 28. januar 2003 til datakrimkonvensjonen. Subsidiært foreslås imidlertid at de deler av denne artikkel som ikke er dekket av eksisterende bestemmelser kan innarbeides med følgende ordlyd:

*§ x Fornektelse, vesentlig minimalisering, aksept eller forsvar av folkemord eller andre forbrytelser mot menneskeheten*

*For krenkende ytring straffes den som setter frem offentlig en ytring som fornekter, vesentlig minimaliserer, aksepterer eller forsvarer folkemord eller andre forbrytelser mot menneskeheten. Likt med en offentlig fremsatt ytring, jf. § 10 andre ledd, regnes en ytring når den er satt frem slik at den er egnet til å nå et større antall personer.*

*Med folkemord og forbrytelser mot menneskeheten menes handlinger som i internasjonal rett og praksis fra anerkjente internasjonale domstoler, er klassifisert som forbrytelser.*

*Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.*

**Til kapitlet om Vern av den personlige frihet og fred**
Nåværende strl § 390 a, som er foreslått videreført som § 26-10, nytt annet ledd skal lyde:

*Atferd som nevnt i første ledd anses forøvet overfor noen også når den er forøvet gjennom bruk av telefon, internett eller annen elektronisk kommunikasjon.*

**Til kapitlet om Vern av tilliten til dokumenter og penger**
*Skisse til enkelte endringer i reglene om dokumentfalsk:*

*§ 31-1 Definisjoner*
*Med bevisbærer menes i dette kapitlet skriftlig dokument, trykt skrift, merke, data eller annet som etter sin art er beregnet på eller egnet til å tjene som bevis.*

*§ 31-2 Særregler for elektronisk signatur*
*Når elektronisk signatur er benyttet, anses objektet alltid som bevisbærer. Elektronisk signatur som uberettiget er påført av uvedkommende, regnes alltid som falsk bevisbærer.*

## 11.4 Endringer i andre lover:

**Markedsføringsloven**
Markedsføringsloven § 2b første ledd skal lyde slik:

Det er forbudt i næringsvirksomhet uten mottakerens forutgående samtykke å rette markedsføringshenvendelser til fysiske personer *ved bruk av* automatisert oppringningssystem (talemaskin).

Markedsføringsloven § 2b tredje, fjerde og femte ledd oppheves.

**Åndsverkloven**
Flertallsforslag:

Åndsverkloven 53a unntatt tredje ledd annet punktum, som foreslås flyttet til en annen paragraf i åndsverkloven, og § 53c oppheves.

## 11.5 Forholdet til straffeloven

De foreslåtte lovbestemmelsene trer istedenfor disse bestemmelsene i straffeloven:

Strl § 145 annet og tredje ledd
Strl § 145b
Strl § 262

De foreslåtte lovbestemmelsene trer delvis istedenfor/overlapper forhold som faller inn under disse bestemmelsene i straffeloven:

Strl § 145 a
Strl § 261
Strl § 393
Strl § 270 første ledd nr 2
Strl § 290
Strl § 317

# Litteraturliste

Adams og Lloyd: Understanding PKI. 2. utgave. Addison-Wesley (USA) 2003.

Andenæs og Bratholm: Spesiell strafferett. 3. utgave. Universitetsforlaget 1996.

Atreya, Hammond, Paine, Starrett og Wu: Digital Signatures. McGraw-Hill (USA) 2003.

Bratholm og Matningsdal: Straffeloven kommentarutgave Bind II. 1. utgave. Universitetsforlaget 1995.

Brownlie, Ian: Principles of Public International Law. Oxford Unversity Press 2003.

Bruce Schneier: Secrets & Lies. Wiley Publishing Inc (USA) 2000.

Feghhi og Williams: Digital Certificates. Addison-Wesley (USA) 1999.

Goldsmith og Wu: Who Controls the Internet? Illusions of a borderless world. Oxford University Press Inc (USA) 2006.

Jansen og Wiese Schartun: Informasjonssikkerhet. Fagbokforlaget 2005.

Lininger og Vines: Phishing. Cutting the Identity Theft Line. Wiley Publishing Inc (USA) 2005.

Matningsdal og Bratholm: Straffeloven Kommentarutgave Bind I. 2. utgave. Universitetsforlaget 2003.

Mirkovic, Dietrich, Dittrich and Reiher: Internet Denial of Service. Pearson Education Inc (USA) 2005.

Møse, Erik: Menneskerettigheter. Cappelen Akademisk Forlag 2002.

Ruud og Ulfstein: Innføring i folkerett. 2. utgave. Universitetsforlaget 2002.

Schjølberg, Stein: Cybercrime: straffbare handlinger mot den alminnelige orden og fred i cyberspace. Cybercrimelaw.net 2006.

Schwaback: Internet and the Law. ABC-CLIO Inc (USA) 2006.

Smith, Grabosky og Urbas: Cyber criminals on Trail. Cambridge University Press (Australia) 2004.

Sunde, Inger Marie: Lov og rett i cyberspace. Fagbokforlaget 2006.

Sunde, Lars Christian: Elektronisk dokumentfalsk. I: Complex 6/04.

Økokrims skriftserie nr. 9/1995: «Datakriminalitet» side 202-210.

**Vedlegg 1**

# Convention on Cybercrime, Budapest, 23.11.2001

### Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

# Konvensjon om datakriminalitet Budapest, 23.11.2001

### Innledning

Medlemsstatene i Europarådet og de andre statene som har undertegnet denne konvensjon,

som tar i betraktning Europarådets mål om å oppnå større enhetlighet mellom sine medlemmer,

som erkjenner verdien av å fremme samarbeidet med de andre statene som er part i denne konvensjon,

som er overbevist om nødvendigheten av å føre og å prioritere en felles kriminalpolitikk som tar sikte på å beskytte samfunnet mot datakriminalitet, blant annet ved å vedta hensiktsmessige lover og å fremme internasjonalt samarbeid,

som er seg bevisst de gjennomgripende forandringer som digitaliseringen, tilnærmingen og den stadige globaliseringen av datanettene har medført,

som er bekymret over faren for at datanettverk og elektroniske data også kan bli brukt til å begå straffbare handlinger og at bevis knyttet til slike handlinger kan lagres og overføres av slike nettverk,

som erkjenner behovet for samarbeid mellom stater og privat industri for å bekjempe datakriminalitet, samt behovet for å beskytte rettmessige interesser i forbindelse med bruk og utvikling av informasjonsteknologi,

som mener at en effektiv kamp mot datakriminalitet krever et sterkere, raskere og mer effektivt internasjonalt samarbeid i straffesaker,

som er overbevist om at denne konvensjon er nødvendig for å forebygge handlinger rettet mot datasystemenes, nettverkenes og dataenes konfidensielle karakter, integritet og tilgjengelighet, samt misbruk av slike systemer, nettverk og data, ved å sørge for kriminalisering av aktivitet som beskrevet i denne konvensjon, samt innføre tilstrekkelig myndighet til å bekjempe slike straffbare handlinger effektivt, ved å tilrettelegge for avdekking, etterforskning og rettslig forfølgning av slike straffbare handlinger både nasjonalt og internasjonalt, og ved å sørge for ordninger som muliggjør et raskt og pålitelig internasjonalt samarbeid,

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 con-

som er seg bevisst behovet for å sikre tilstrekkelig balanse mellom hensynet til håndhevelse av loven og overholdelse av de grunnleggende menneskerettigheter, nedfelt i Europarådets konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter av 1950, De forente nasjoners internasjonale konvensjon om sivile og politiske rettigheter av 1966, samt andre internasjonale traktater om menneskerettigheter som får anvendelse og som bekrefter ethvert menneskes rett til fritt å kunne ha sine egne meninger, samt retten til ytringsfrihet, herunder frihet til å søke, motta og meddele opplysninger og ideer av alle slag, uavhengig av grenser, samt retten til respekt for privatlivets fred,

som også er seg bevisst retten til vern av personopplysninger, nedfelt i Europarådets konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger av 1981,

som tar i betraktning De forente nasjoners konvensjon om barnets rettigheter av 1989 og Den internasjonale arbeidsorganisasjonens konvensjon om de verste former for barnearbeid av 1999,

som tar hensyn til Europarådets eksisterende konvensjoner om samarbeid på det strafferettslige området samt liknende traktater inngått mellom Europarådets medlemsstater og andre stater, og som understreker at denne konvensjon er ment å utfylle de nevnte konvensjonene med det mål å gjøre strafferettslig etterforskning og forfølgning mer effektiv samt gjøre det mulig å innhente elektroniske bevis i forbindelse med straffbare handlinger,

som gleder seg over utviklingen i den senere tid, som ytterligere fremmer internasjonal forståelse og samarbeid når det gjelder bekjempelse av datakriminalitet, herunder tiltak truffet av De forente nasjoner, OECD, Den europeiske union og G8,

som minner om anbefaling nr. R (85) 10 om den praktiske håndhevelse av Den europeiske konvensjon om gjensidig samarbeid i straffesaker når det gjelder rettsanmodninger om overvåking av telekommunikasjon, anbefaling nr. R (88) 2 om piratvirksomhet knyttet til opphavsrett og beslektede rettigheter, anbefaling nr. R (87) 15 om regulering av bruk av personopplysninger innenfor politisektoren, anbefaling nr. R (95) 4 om beskyttelse av personopplysninger innenfor telekommunikasjonstjenester, særlig telefontjenester, samt anbefaling nr. R (89) 9 om kriminalitet knyttet til datamaskiner, som gir retningslinjer for definering av visse typer datakriminalitet i nasjonal rett, og anbefaling nr. R

cerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

(95) 13 om problemer i straffeprosesslovgivningen knyttet til informasjonsteknologi,

som viser til resolusjon nr. 1 vedtatt av de europeiske justisministrene under deres 21. konferanse (Praha, juni 1997), som anbefalte Ministerkomiteen å støtte arbeidet med datakriminalitet i Den europeiske komité for kriminalspørsmål (CDPC) for å få til en tilnærming av bestemmelsene i de ulike nasjonale straffelovgivninger, samt tillate bruk av effektive midler i etterforskning av slike straffbare handlinger, samt resolusjon nr. 3, vedtatt under de europeiske justisministrenes 23. konferanse (London, juni 2000), som oppfordret forhandlingspartene til å fortsette arbeidet for å finne egnede løsninger, slik at et størst mulig antall stater kan bli part i konvensjonen, og som erkjente behovet for en rask og effektiv internasjonal samarbeidsordning, der det tas behørig hensyn til de særlige krav som stilles i kampen mot datakriminalitet,

som også tar i betraktning handlingsplanen vedtatt av Europarådets stats- og regjeringssjefer under deres annet toppmøte (Strasbourg, 10. og 11. oktober 1997), for å finne fram til felles mottiltak basert på Europarådets normer og verdier for å møte utviklingen av ny informasjonsteknologi,

er blitt enige om følgende:

## Chapter I – Use of terms

*Article 1 – Definitions*

For the purposes of this Convention:

a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c) "service provider" means:
   i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
   ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d) "traffic data" means any computer data relating to a communication by means of a computer

## Kapittel I - Termbruk

*Artikkel 1 - Definisjoner*

I forbindelse med denne konvensjon betyr:

a) «datasystemer»: enhver innretning eller gruppe innretninger som er koplet sammen eller som hører sammen, hvorav en eller flere utfører programmert, automatisk behandling av data,

b) «elektroniske data»: enhver framstilling av fakta, informasjon eller begrep i en form som er egnet for behandling i et datasystem, herunder et program som kan få et datasystem til å utføre en funksjon,

c) «tjenesteyter»:
   i. en offentlig eller privat virksomhet som gir brukere av sine tjenester muligheten til å kommunisere ved hjelp av et datasystem, og
   ii. enhver annen virksomhet som behandler eller lagrer elektroniske data på vegne av en slik kommunikasjonstjeneste eller brukere av slike tjenester.

d) «trafikkdata»: alle elektroniske data knyttet til en kommunikasjon via et datasystem som er

system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

blitt produsert av et datasystem som inngikk i kommunikasjonskjeden, og som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet eller type underliggende tjeneste.

## Chapter II – Measures to be taken at the national level

## Kapittel II - Tiltak som skal iverksettes nasjonalt

### Section 1 – Substantive criminal law

### Avsnitt 1 - Materiell strafferett

### Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

### Del 1 - Straffbare handlinger som rammer datasystemers og dataenes fortrolige karakter, integritet og tilgjengelighet

*Article 2 – Illegal access*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

*Artikkel 2 - Ulovlig tilgang*

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå forsettlig, urettmessig tilgang til hele eller deler av et datasystem som straffbar handling etter nasjonal rett. En part kan stille som vilkår at den straffbare handlingen er begått ved brudd på sikkerhetstiltak i den hensikt å få tak i elektroniske data eller i annen uredelig hensikt, eller i forbindelse med et datasystem som er knyttet til et annet datasystem.

*Article 3 – Illegal interception*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

*Artikkel 3 - Ulovlig oppfanging av data*

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbar handling etter nasjonal rett, forsettlig, urettmessig oppfanging av elektroniske data med tekniske midler i forbindelse med ikke offentlig tilgjengelige overføringer til, fra eller innenfor et datasystem, herunder elektromagnetisk stråling fra datasystemer som inneholder slike elektroniske data. En part kan stille som vilkår at den straffbare handlingen er begått med uredelig hensikt, eller i forbindelse med et datasystem som er knyttet til et annet datasystem.

*Article 4 – Data interference*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

*Artikkel 4 - Inngrep i dataenes integritet*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå forsettlig ødeleggelse, sletting, forringelse, endring eller fjerning av elektroniske data som straffbare handlinger etter nasjonal rett.

2. En part kan forbeholde seg retten til å stille som vilkår at handlingen beskrevet i nr. 1 medfører alvorlig skade.

*Article 5 – System interference*

Each Party shall adopt such legislative and other measures as may be necessary to establish as

*Artikkel 5 - Inngrep i driften av et datasystem*

Hver part skal vedta de lover og andre tiltak som er nødvendige for å fastslå at følgende forsettlige,

criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

urettmessige og alvorlige handlinger, som forhindrer et datasystems drift, er straffbare handlinger etter nasjonal rett: tilførsel, overføring, ødeleggelse, sletting, forringelse og endring eller fjerning av data.

*Article 6 – Misuse of devices*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   a) the production, sale, procurement for use, import, distribution or otherwise making available of:
      i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
      ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
   b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

*Artikkel 6 - Misbruk av innretninger og tilgangsdata*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå følgende forsettlige og urettmessige handlinger som straffbare handlinger etter nasjonal rett

   a) produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte av:
      i. en innretning, herunder et dataprogram, utviklet eller tilpasset hovedsakelig i den hensikt å begå en av de straffbare handlingene fastslått i samsvar med artikkel 2 til 5,
      ii. et passord, adgangskode eller liknende data som gir tilgang til hele eller deler av et datasystem, i den hensikt å bruke det til å begå en av de straffbare handlingene fastslått i artikkel 2 til 5, og

   b) besittelse av utstyr og adgangskoder omhandlet i bokstav a) i) eller ii) ovenfor i den hensikt å bruke det for å begå de straffbare handlingene fastslått i artikkel 2 til 5. En part kan i sin nasjonale rett stille vilkår om besittelse av slikt utstyr eller slike adgangskoder i et visst omfang før det får strafferettslige følger.
2. Denne artikkel skal ikke tolkes slik at produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte eller besittelse omhandlet i nr. 1 i denne artikkel medfører strafferettslig ansvar når det ikke skjer i den hensikt å begå en straffbar handling fastslått i samsvar med artikkel 2 til 5 i denne konvensjon, som autorisert testing og beskyttelse av et datasystem.
3. Hver part kan forbeholde seg retten til ikke å anvende nr. 1 i denne artikkel, forutsatt at forbeholdet ikke gjelder salg, distribusjon eller tilgjengeliggjøring på annen måte av utstyret og adgangskodene omhandlet i nr. 1 bokstav a) ii)

## Title 2 – Computer-related offences

*Article 7 – Computer-related forgery*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

*Article 8 – Computer-related fraud*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data,
b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

## Title 3 – Content-related offences

*Article 9 – Offences related to child pornography*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   a) producing child pornography for the purpose of its distribution through a computer system;
   b) offering or making available child pornography through a computer system;
   c) distributing or transmitting child pornography through a computer system;
   d) procuring child pornography through a computer system for oneself or for another person;
   e) possessing child pornography in a computer system or on a computer-data storage medium.

## Del 2 - Straffbare handlinger knyttet til datamaskiner

*Artikkel 7 - Datarelatert falsk*

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbare handlinger etter nasjonal rett, forsettlig, urettmessig tilførsel, endring, sletting eller fjerning av elektroniske data som fører til ugyldige data, i den hensikt at de skal anses som eller brukes i rettslig sammenheng som om de var ekte, enten de er direkte lesbare og forståelige eller ikke. En part kan stille som vilkår at det må foreligge svikaktig eller annen uredelig hensikt før straffansvar pådras.

*Artikkel 8 - Datarelatert bedrageri*

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbare handlinger etter nasjonal rett, forsettlige, urettmessige handlinger som påfører andre tap av eiendom gjennom:

a) innlegging, endring, sletting eller utilgjengeliggjøring av elektroniske data,
b) inngrep som forstyrrer et datasystems drift, i den svikaktige eller uredelige hensikt å skaffe seg selv eller andre urettmessig økonomisk vinning.

## Del 3 - Straffbare handlinger knyttet til innhold

*Artikkel 9 - Straffbare handlinger knyttet til barnepornografi*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå følgende forsettlig og urettmessig aktivitet som straffbar handling etter nasjonal rett:

   a) å produsere barnepornografi for distribusjon via et datasystem,

   b) å tilby eller gjøre barnepornografi tilgjengelig via et datasystem,
   c) å distribuere eller formidle barnepornografi via et datasystem,
   d) å skaffe til veie barnepornografi til seg selv eller andre via et datasystem,

   e) å være i besittelse av barnepornografi lagret i et datasystem eller på et annet datalagringsmedium.

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
   a) a minor engaged in sexually explicit conduct;
   b) a person appearing to be a minor engaged in sexually explicit conduct;
   c) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

## Title 4 – Offences related to infringements of copyright and related rights

*Article 10 – Offences related to infringements of copyright and related rights*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Uttrykket «barnepornografi» i nr. 1 ovenfor skal omfatte pornografisk materiale som gir en visuell framstilling av:
   a) en mindreårig som er involvert i eksplisitt seksuell aktivitet,
   b) en person som ser ut som en mindreårig som er involvert i eksplisitt seksuell aktivitet,
   c) realistiske bilder som framstiller en mindreårig som er involvert i eksplisitt seksuell aktivitet.
3. Uttrykket «mindreårig» i nr. 2 ovenfor skal omfatte alle personer under 18 år. En part kan imidlertid oppstille en lavere aldersgrense, som ikke skal være under 16 år.

4. Hver part kan forbeholde seg retten til ikke å anvende hele eller deler av nr. 1 d) og e), samt nr. 2 b) og c).

## Del 4 - Straffbare handlinger knyttet til krenkelser av opphavsrett og nærstående rettigheter

*Artikkel 10 - Straffbare handlinger knyttet til krenkelse av opphavsrett og nærstående rettigheter*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å kunne fastslå som straffbar handling etter nasjonal rett, en krenkelse av opphavsretten slik den er definert i vedkommende parts rett i samsvar med de forpliktelser parten har påtatt seg etter Parisakten av 24. juli 1971 til Bernkonvensjonen for vern av litterære og kunstneriske verk, Avtalen om handelsrelaterte sider ved immaterielle rettigheter og WIPO-traktaten om opphavsrett, med unntak av enhver åndsrett fastsatt i disse konvensjonene, når slike handlinger begås med forsett, i et kommersielt omfang og ved hjelp av et datasystem.
2. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbar handling etter nasjonal rett, en krenkelse av nærstående rettigheter slik de er definert i vedkommende parts rett i samsvar med de forpliktelser parten har påtatt seg etter Den internasjonale konvensjon om vern for utøvende kunstnere, fonogramprodusenter og kringkastingsinstitusjoner (Romakonvensjonen), Avtalen om handelsrelaterte sider ved immaterielle rettigheter og WIPO-traktaten om kunstneriske framføringer og fonogrammer, med unntak av enhver åndsrett fastsatt i disse konvensjonene, når slike handlinger begås med forsett, i et kommersielt omfang og ved hjelp av et datasystem.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

## Title 5 – Ancillary liability and sanctions

*Article 11 – Attempt and aiding or abetting*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

*Article 12 – Corporate liability*

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

   a) a power of representation of the legal person;
   b) an authority to take decisions on behalf of the legal person;
   c) an authority to exercise control within the legal person.
2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible

3. En part kan forbeholde seg retten til ikke å ilegge strafferettslig ansvar etter nr. 1 og 2 i begrensede tilfeller, forutsatt at det finnes andre effektive rettsmidler, og at slikt forbehold ikke innskrenker partens internasjonale forpliktelser i henhold til de internasjonale instrumentene nevnt i nr. 1 og 2 i denne artikkel.

## Del 5 - Andre former for ansvar og straffereaksjoner

*Artikkel 11 - Forsøk og medvirkning*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbar handling etter nasjonal rett, forsettlig medvirkning til en handling etter artikkel 2 til 10 i denne konvensjon når slik medvirkning skjer i den hensikt å begå slik handling.

2. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som en straffbar handling etter nasjonal rett, forsettlig forsøk på å begå en av de straffbare handlingene omhandlet i artikkel 3 til 5, 7, 8, 9 nr. 1 a) og c) i denne konvensjonen

3. Hver part kan forbeholde seg retten til ikke å anvende i sin helhet eller delvis nr. 2 i denne artikkel.

*Artikkel 12 - Juridiske personers ansvar*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre at en juridisk person kan holdes ansvarlig for straffbare handlinger fastsatt i samsvar med denne konvensjon, som er begått til den juridiske personens fordel av en fysisk person som opptrer enten på egen hånd eller som en del av et organ tilhørende vedkommende juridiske person, og som har en ledende stilling i henhold til:
   a) fullmakt til å representere den juridiske personen,
   b) myndighet til å treffe beslutninger på vegne av den juridiske personen, eller
   c) myndighet til å utøve kontroll innenfor den juridiske personen,
2. I tillegg til de tilfeller som er fastsatt i nr. 1, skal hver part treffe nødvendige tiltak for å sikre at en juridisk person kan holdes ansvarlig dersom manglende tilsyn eller kontroll fra en fysisk persons side nevnt i nr. 1 har gjort det mulig å begå en straffbar handling fastsatt i samsvar

the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

med denne konvensjon til fordel for den juridiske personen.

3. Avhengig av partens rettsprinsipper, kan den juridiske personens ansvar være strafferettslig, sivilrettslig eller administrativt.
4. Slikt ansvar skal ikke berøre det strafferettslige ansvar som påhviler fysiske personer som har begått den straffbare handlingen.

*Article 13 – Sanctions and measures*

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

*Artikkel 13 - Straffereaksjoner og tiltak*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre at straffbare handlinger fastsatt i samsvar med artikkel 2 til 11 kan straffes med effektive, forholdsmessige og forebyggende straffereaksjoner, som også omfatter frihetsstraff.
2. Hver part skal sikre at juridiske personer som holdes ansvarlig i samsvar med artikkel 12, skal kunne straffes med effektive, forholdsmessige og avskrekkende straffereaksjoner eller ikke-strafferettslige sanksjoner, herunder økonomiske sanksjoner.

## Section 2 – Procedural law

## Avsnitt 2. Prosesslovgivning

### Title 1 – Common provisions

### Del 1 - Felles bestemmelser

*Article 14 – Scope of procedural provisions*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
   a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   b) other criminal offences committed by means of a computer system; and
   c) the collection of evidence in electronic form of a criminal offence.
3. 
   a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the

*Artikkel 14 Prosessbestemmelsenes virkeområde*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å innføre de fullmakter og prosedyrer som er fastsatt i dette avsnittet med henblikk på en bestemt strafferettslig etterforskning eller forfølgning.
2. Med unntak for de tilfeller som er særskilt angitt i artikkel 21, skal hver part anvende fullmaktene og prosedyrene nevnt i nr. 1 i forbindelse med:
   a) straffbare handlinger fastsatt i samsvar med artikkel 2 til 11 i denne konvensjon,
   b) andre straffbare handlinger begått ved hjelp av et datasystem, og
   c) innhenting av elektroniske bevis for en straffbar handling.
3. 
   a) Hver part kan forbeholde seg retten til å anvende tiltakene nevnt i artikkel 20 bare for de straffbare handlingene eller kategoriene straffbare handlinger som er angitt i forbeholdet, forutsatt at spekteret av slike straffbare handlinger eller kategorier straffbare handlinger ikke er mer begrenset enn

measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
   i. is being operated for the benefit of a closed group of users, and
   ii. does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

spekteret av straffbare handlinger som parten anvender tiltakene nevnt i artikkel 21 på. Hver part skal overveie å begrense et slikt forhold slik at tiltaket nevnt i artikkel 20 kan få videst mulig anvendelse.

b) Når en part på grunn av begrensninger i sin lovgivning på det tidspunkt denne konvensjon blir vedtatt ikke er i stand til å anvende tiltakene nevnt i artikkel 20 og 21 for kommunikasjoner som overføres med et datasystem tilhørende en tjenesteyter,

   i. som drives til fordel for en lukket brukergruppe, og
   ii. som ikke bruker offentlige kommunikasjonsnett og ikke er tilknyttet et annet, verken offentlig eller privat datasystem, kan denne parten forbeholde seg retten til ikke å anvende disse tiltakene for slike kommunikasjoner. Hver part skal overveie å begrense et slikt forbehold slik at tiltakene nevnt i artikkel 20 og 21 kan få videst mulig anvendelse.

*Article 15 – Conditions and safeguards*

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

*Artikkel 15 - Vilkår og rettssikkerhetsgarantier*

1. Hver part skal sikre at innføringen, iverksettelsen og anvendelsen av fullmaktene og prosedyrene fastsatt i dette avsnitt er underlagt vilkårene og rettssikkerhetsgarantiene fastsatt i partens nasjonale rett, som skal sikre tilstrekkelig beskyttelse av menneskerettighetene og frihetene, herunder rettighetene som følger av de forpliktelser parten har påtatt seg etter Europarådets konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter av 1950, De forente nasjoners internasjonale konvensjon om sivile og politiske rettigheter av 1966 og andre internasjonale menneskerettighetsinstrumenter, og som skal omfatte forholdsmessighetsprinsippet.
2. Dersom det er hensiktsmessig ut fra den berørte prosedyren eller fullmaktens karakter, skal slike vilkår og garantier blant annet omfatte rettslig og annet uavhengig tilsyn, grunner som rettferdiggjør anvendelse og begrensning av omfanget eller gyldighetstiden for slike fullmakter eller prosedyrer.
3. I den utstrekning det er forenlig med allmennhetens interesser, særlig forsvarlig rettspleie, skal en part vurdere hvilken virkning fullmaktene og prosedyrene i dette avsnittet vil få på tredjeparters rettigheter, ansvar og legitime interesser.

## Title 2 – Expedited preservation of stored computer data

*Article 16 – Expedited preservation of stored computer data*

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

*Article 17 – Expedited preservation and partial disclosure of traffic data*

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
   a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
   b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

## Del 2 - Hurtig sikring av lagrede, elektroniske data

*Artikkel 16 - Hurtig sikring av lagrede, elektroniske data*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gjøre sine kompetente myndigheter i stand til å beordre eller på annen måte sørge for hurtig sikring av nærmere angitte elektroniske data, herunder trafikkdata, som er blitt lagret i et datasystem, særlig når det er grunn til å tro at de elektroniske dataene er spesielt utsatt for tap eller endring.
2. Når en part iverksetter nr. 1 ovenfor ved å gi ordre til en person om å sikre nærmere angitte lagrede elektroniske data som denne personen har i sin besittelse eller har kontroll over, skal parten vedta slike lover og andre tiltak som eventuelt er nødvendige for å pålegge denne personen å sikre og beskytte disse dataenes integritet i det tidsrom som er nødvendig, inntil 90 dager maksimum, slik at de kompetente myndigheter skal ha mulighet til å be om at de utleveres. En part kan sørge for at et slikt pålegg siden forlenges.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å pålegge den som oppbevarer dataene eller annen person som skal utføre sikring, taushetsplikt med hensyn til iverksettelsen av slike prosedyrer i det tidsrom som partens nasjonale rett gir hjemmel for.
4. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

*Artikkel 17 - Hurtig sikring og delvis utlevering av trafikkdata*

1. Hver part skal med hensyn til trafikkdata som skal sikres i henhold til artikkel 16, vedta de lover og andre tiltak som eventuelt er nødvendige for å:
   a) sikre at slik hurtig sikring av trafikkdata er mulig uansett om en eller flere tjenesteytere var involvert i overføringen av den aktuelle kommunikasjon,
   b) sikre hurtig utlevering til partens kompetente myndighet eller til en person utpekt av denne myndighet av en tilstrekklig mengde data til at parten kan identifisere tjenesteyterne og kommunikasjonsruten.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### Title 3 – Production order

*Article 18 – Production order*

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
   a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

   b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   a) the type of communication service used, the technical provisions taken thereto and the period of service;
   b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

   c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

### Title 4 – Search and seizure of stored computer data

*Article 19 – Search and seizure of stored computer data*

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

2. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

### Del 3 - Pålegg om utlevering av data

*Artikkel 18 - Pålegg om utlevering av data*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å pålegge:
   a) en person som befinner seg på dens territorium, å utlevere nærmere angitte elektroniske data som denne personen har i sin besittelse eller har kontroll over, og som ligger lagret i et datasystem eller på et datalagringsmedium, og
   b) en tjenesteyter som tilbyr sine tjenester på partens territorium, å framlegge abonnentopplysninger knyttet til slike tjenester som denne tjenesteyteren har i sin besittelse eller har kontroll over.
2. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.
3. «Abonnentopplysninger» i denne artikkel betyr enhver opplysning i form av elektroniske data eller annen form som en tjenesteyter har i sin besittelse og som gjelder abonnentene av slike tjenester, unntatt data som gjelder trafikk eller innhold som gjør det mulig å fastslå:

   a) hvilke type kommunikasjonstjeneste som er benyttet, hvilke tekniske tiltak som er truffet i den forbindelse og tjenestens varighet,
   b) abonnentens identitet, postadresse eller geografiske adresse, telefonnummer og andre numre for tilgang, opplysninger om fakturering og betaling som er tilgjengelige i henhold til inngått kontrakt eller ordning angående tjenesten,
   c) enhver annen opplysning på stedet der kommunikasjonsutstyret er installert, som er tilgjengelig i henhold til inngått kontrakt eller ordning angående tjenesten.

### Del 4 - Ransaking og beslag av lagrede, elektroniske data

*Artikkel 19 - Ransaking og beslag av lagrede, elektroniske data*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å ransake eller på annen måte få tilgang til:

a) computer system or part of it and computer data stored therein; and

b) a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
   a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
   b) make and retain a copy of those computer data;
   c) maintain the integrity of the relevant stored computer data;
   d) render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## Title 5 – Real-time collection of computer data

*Article 20 – Real-time collection of traffic data*

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
   a) collect or record through the application of technical means on the territory of that Party, and

a) et datasystem eller del av slikt datasystem, samt elektroniske data lagret i datasystemet, og
b) datalagringsmedium der elektroniske data kan lagres, på partens territorium.

2. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre at dets myndigheter, når de ransaker eller på annen måte får tilgang til et bestemt datasystem eller del av det i samsvar med nr. 1 a) og har grunn til å tro at de ettersøkte dataene er lagret i et annet datasystem eller del av det på sitt territorium, og disse data er lovlig tilgjengelige fra eller for det første systemet, har mulighet til raskt å utvide ransakingen eller annen tilgang til dette andre systemet.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å beslaglegge eller på annen måte sikre elektroniske data som de har fått tilgang til i samsvar med nr. 1 eller 2. Disse tiltakene skal omfatte fullmakt til å:
   a) beslaglegge eller på annen måte sikre et datasystem eller del av det, eller et datalagringsmedium,
   b) lage eller beholde et kopi av disse elektroniske dataene,
   c) bevare de relevante, elektronisk lagrede dataenes integritet, og
   d) gjøre utilgjengelige eller fjerne disse elektroniske dataene i det aktuelle datasystem.
4. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å pålegge en person som har kjennskap til driften av et datasystem eller tiltak som anvendes for å beskytte de elektroniske data i systemet, i rimelig utstrekninig å gi de nødvendige opplysninger som gjør det mulig å iverksette tiltakene omhandlet i nr. 1 og 2.
5. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

## Del 5 - Innhenting av elektroniske data i sanntid

*Artikkel 20 - Innhenting av trafikkdata i sanntid*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å:
   a) innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, og

b) compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party; or
ii. to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

b) pålegge en tjenesteyter, så langt tjenesteyterens eksisterende tekniske midler tillater, å:
i. innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, eller
ii. å samarbeide og hjelpe de kompetente myndigheter å innhente eller lagre

i sanntid trafikkdata som er knyttet til bestemte kommunikasjoner på partens territorium og som er overført ved hjelp av et datasystem.

2. Når en part som følge av etablerte prinsipper i sitt nasjonale rettssystem ikke kan innføre tiltakene omhandlet i nr. 1 a), kan den i stedet vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre innhenting eller lagring i sanntid av trafikkdata knyttet til bestemte kommunikasjoner på sitt territorium ved hjelp av tekniske midler på dette territorium.

3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å pålegge en tjenesteyter taushetsplikt med hensyn til iverksettelsen av tvangsmidlene fastsatt i denne artikkel, samt enhver opplysning i denne sammenheng.
4. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

*Article 21 – Interception of content data*

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party, or
ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

*Artikkel 21 - Oppfanging av data knyttet til innhold*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt i forbindelse med et spekter av alvorlige straffbare handlinger som defineres i partens nasjonale rett, til i sanntid å:
a) innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, og

b) pålegge en tjenesteyter, så langt tjenesteyterens eksisterende tekniske midler tillater, å:
i. innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, eller
ii. samarbeide og hjelpe de kompetente myndigheter å innhente eller lagre

data knyttet til innholdet i bestemte kommunikasjoner på partens territorium, og som er overført ved hjelp av et datasystem.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## Section 3 – Jurisdiction

*Article 22 – Jurisdiction*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

   a) in its territory; or
   b) on board a ship flying the flag of that Party; or
   c) on board an aircraft registered under the laws of that Party; or
   d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accor-

2. Når en part som følge av etablerte prinsipper i sitt nasjonale rettssystem ikke kan innføre tiltakene omhandlet i nr. 1 a), kan den i stedet vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre innhenting eller lagring i sanntid av data knyttet til innholdet i bestemte kommunikasjoner på sitt territorium ved hjelp av tekniske midler på dette territorium.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å pålegge en tjenesteyter taushetsplikt med hensyn til iverksettelsen av fullmaktene fastsatt i denne artikkel, samt enhver opplysning i denne sammenheng.
4. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

## Avsnitt 3 - Jurisdiksjon

*Artikkel 22 - Jurisdiksjon*

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å etablere jurisdiksjon med hensyn til enhver straffbar handling fastslått i samsvar med artikkel 2 til 11 i denne konvensjon, når den straffbare handlingen er begått:
   a) på denne partens territorium, eller
   b) om bord på et skip som fører denne partens flagg, eller
   c) om bord på et luftfartøy som er registrert etter denne partens rett, eller
   d) av en borger av denne part dersom handlingen kan straffes på det sted handlingen ble begått, eller dersom den straffbare handlingen er begått utenfor enhver stats territoriale jurisdiksjon.
2. Hver stat kan forbeholde seg retten til ikke å anvende eller til bare å anvende i bestemte tilfeller eller på bestemte vilkår reglene om jurisdiksjon fastsatt i nr. 1 b) til d) i denne artikkel eller deler av disse.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå jurisdiksjon med hensyn til de straffbare handlingene omhandlet i artikkel 24 nr. 1 i denne konvensjon, når den antatte gjerningsmann befinner seg på partens territorium og parten ikke utleverer vedkommende til en annen part utelukkende av hensyn til vedkommendes nasjonalitet, etter en anmodning om utlevering.
4. Denne konvensjon utelukker ikke strafferettslig jurisdiksjon som utøves i samsvar med nasjonal rett.
5. Når mer enn en part gjør krav på jurisdiksjon med hensyn til en påstått straffbar handling

dance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

fastslått i samsvar med denne konvensjon, skal de berørte parter, når det er hensiktsmessig, rådføre seg med hverandre for å bestemme hvilken jurisdiksjon som er best egnet til å gjennomføre rettsforfølgningen.

## Chapter III – International co-operation

## Kapittel III - Internasjonalt samarbeid

### Section 1 – General principles

### Avsnitt 1 - Generelle prinsipper

### Title 1 – General principles relating to international co-operation

### Del 1 - Generelle prinsipper angående internasjonalt samarbeid

*Article 23 – General principles relating to international co-operation*

*Artikkel 23 - Generelle prinsipper angående internasjonalt samarbeid*

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Partene skal samarbeide i samsvar med bestemmelsene i dette kapittel og ved å anvende de relevante internasjonale instrumentene om internasjonalt samarbeid i straffesaker, ordninger basert på felles eller gjensidig lovgivning og nasjonal rett, i størst mulig utstrekning med henblikk på etterforskning eller forfølgning av straffbare handlinger knyttet til datasystemer og data, eller for innhenting av elektroniske bevis for en straffbar handling.

### Title 2 – Principles relating to extradition

### Del 2 - Prinsipper angående utlevering

*Article 24 – Extradition*

*Artikkel 24 - Utlevering*

1.
   a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
   b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

1.
   a) Denne artikkel gjelder utlevering mellom partene som følge av straffbare handlinger fastslått i samsvar med artikkel 2 til 11 i denne konvensjon, forutsatt at de etter begge de berørte partenes rett kan straffes med en maksimum frihetsstraff på minst ett år, eller med en strengere straff.

   b) Dersom det kreves en annen minimumsstraff i henhold til en ordning basert på en felles eller gjensidig lovgivning eller en utleveringsavtale, herunder Den europeiske konvensjon om utlevering (ETS nr. 24), inngått mellom to eller flere parter, skal minstestraffen fastsatt i et slik ordning eller avtale få anvendelse.
2. De straffbare handlingene beskrevet i nr. 1 i denne artikkel skal anses å inngå blant de straffbare handlinger som gir grunnlag for utlevering i enhver eksisterende utleveringsavtale mellom to eller flere parter. Partene forplikter seg til å inkludere slike straffbare handlinger blant straffbare handlinger som gir grunnlag for utlevering i enhver utleveringsavtale som vil bli inngått mellom to eller flere parter.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.
5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7.
   a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
   b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

**Title 3 – General principles relating to mutual assistance**

*Article 25 – General principles relating to mutual assistance*

1. The Parties shall afford one another mutual assistance to the widest extent possible for the

3. Dersom en part som stiller som vilkår for utlevering at det foreligger en avtale, mottar en anmodning om utlevering fra en annen part som den ikke har noen utleveringsavtale med, kan den betrakte denne konvensjon som rettslig grunnlag for utlevering for straffbare handlinger nevnt i nr. 1 i denne artikkel.
4. Parter som ikke stiller som vilkår for utlevering at det foreligger en avtale, skal anerkjenne de straffbare handlingene nevnt i nr. 1 i denne artikkel som straffbare handlinger som gir grunnlag for utlevering mellom dem.
5. Utlevering skal skje på de vilkår som er fastsatt i den anmodede parts rett eller i gjeldende utleveringsavtaler, herunder de grunner den anmodede part kan påberope seg for å avslå utlevering.
6. Dersom utlevering for en straffbar handling nevnt i nr. 1 i denne artikkel avslås utelukkende på grunnlag av den ettersøkte personens nasjonalitet, eller fordi den anmodede part mener at den har jurisdiksjon med hensyn til den straffbare handlingen, skal den anmodede part, etter anmodning fra den anmodende part, forelegge saken for sine kompetente myndigheter med henblikk på rettslig forfølgning, og skal innen rimelig tid avgi rapport om det endelige resultatet til den anmodende part. Disse myndighetene skal treffe sin avgjørelse og utføre sin etterforskning og rettslige forfølgning på samme måte som ved enhver annen straffbar handling av tilsvarende karakter etter denne partens rett.

7.
   a) Hver part skal ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument meddele Europarådets generalsekretær navnet og adressen på hver myndighet som har ansvaret for å oversende eller motta en anmodning om utlevering eller midlertidig pågripelse dersom det ikke foreligger noen avtale.
   b) Europarådets generalsekretær skal sette opp og holde oppdatert et register over myndigheter som slik er utpekt av partene. Hver part skal sikre at opplysningene i registeret til enhver tid er riktige.

**Del 3 - Generelle prinsipper angående gjensidig hjelp**

*Artikkel 25 - Generelle prinsipper angående gjensidig hjelp*

1. Partene skal gi hverandre gjensidig hjelp i størst mulig utstrekning i forbindelse med et-

purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

terforskning eller rettslig forfølgning av straffbare handlinger knyttet til datasystemer og data, eller med innhenting av elektroniske bevis for en straffbar handling.

2. Hver part kan også vedta de lover og andre tiltak som eventuelt er nødvendige for å gjennomføre forpliktelsene fastsatt i artikkel 27 til 35.

3. Hver part kan i hastetilfeller sende anmodninger om gjensidig hjelp eller meddelelser om slik hjelp ved hjelp av raske kommunikasjonsmidler, herunder faks eller e-post, i den utstrekning slike midler gir tilstrekkelig sikkerhet og autentifisering (herunder bruk av kryptering der det er nødvendig), med ettersendelse av formell bekreftelse dersom den anmodede part krever det. Den anmodede part skal godta og besvare anmodningen som oversendes med slike raske kommunikasjonsmidler.

4. Unntatt når annet er spesielt angitt i artiklene i dette kapittel, skal gjensidig hjelp være underlagt vilkårene fastsatt i den anmodede parts rett eller i gjeldende avtaler om gjensidig hjelp, herunder de grunner den anmodede part eventuelt påberoper seg for å avslå samarbeid. Den anmodede part skal ikke bruke retten til å avslå gjensidig hjelp i forbindelse med de straffbare handlingene nevnt i artikkel 2 til 11 utelukkende på grunnlag av at anmodningen gjelder en straffbar handling som den anser som en fiskal forbrytelse.
5. Dersom den anmodede part i samsvar med bestemmelsene i dette kapittel har adgang til å stille som vilkår for gjensidig hjelp at det foreligger dobbel straffbarhet, skal dette vilkåret anses oppfylt, uansett om partens lover plasserer den straffbare handlingen i samme kategori straffbare handlinger eller bruker samme betegnelse for den straffbare handlingen som den anmodende part eller ikke, dersom atferden som ligger til grunn for forbrytelsen som det søkes om hjelp for, er en straffbar handling etter denne partens lover.

*Article 26 – Spontaneous information*

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accor-

*Artikkel 26 - Uoppfordret formidling av opplysninger*

1. En part kan i den grad nasjonal rett tillater og uten å ha mottatt anmodning om det på forhånd oversende en annen part opplysninger den har mottatt i forbindelse med egen etterforskning når den mener at kjennskap til slike opplysninger kan hjelpe mottakerparten med å innlede eller gjennomføre etterforskning eller rettslig forfølgning av straffbare handlinger etter den-

dance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

ne konvensjon, eller kan føre til, en anmodning fra den andre parten om samarbeid i henhold dette kapittel.

2. Parten som oversender slike opplysninger, kan før oversendelse kreve at opplysningene skal behandles fortrolig eller bare brukes på bestemte vilkår. Dersom mottakerparten ikke kan etterkomme en slik anmodning, skal den underrette parten som oversender opplysningene, som så skal avgjøre om opplysningene likevel bør oversendes. Dersom mottakerparten mottar opplysningene på bestemte vilkår, skal den være bundet av vilkårene.

### Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

*Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements*

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2.
   a) Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
   b) The central authorities shall communicate directly with each other;
   c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
   d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

### Del 4 - Framgangsmåter ved anmodning om gjensidig bistand når det ikke foreligger gjeldende internasjonale avtaler

*Artikkel 27 - Framgangsmåter ved anmodning om gjensidig hjelp når det ikke foreligger gjeldende internasjonale avtaler*

1. Dersom det ikke foreligger noen avtale eller ordning om gjensidig bistand basert på gjeldende felles eller gjensidig lovgivning mellom den anmodende og den anmodede part, skal bestemmelsene i nr. 2 til 10 i denne artikkel gjelde. Bestemmelsene i denne artikkel får ikke anvendelse når en slik avtale, ordning eller lovgivning finnes, med mindre de berørte partene bestemmer å anvende i stedet hele eller deler av resten av denne artikkel.
2.
   a) Hver part skal utpeke en sentral myndighet eller sentrale myndigheter som skal ha ansvaret for å oversende og svare på anmodninger om gjensidig bistand, å gjennomføre slike anmodninger, eller videreformidle dem til de kompetente myndigheter for gjennomføring.
   b) De sentrale myndigheter skal kommunisere med hverandre direkte.
   c) Hver part skal ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennelses- eller tiltredelsesdokument meddele Europarådets generalsekretær navnet og adressen til myndighetene utpekt i henhold til dette nummer.
   d) Europarådets generalsekretær skal sette opp og holde oppdatert et register over sentrale myndigheter som er utpekt av partene. Hver part skal sikre at opplysningene i registeret til enhver tid er riktige.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
   a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

   b) it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
9.
   a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the

3. Anmodninger om gjensidig bistand etter denne artikkel skal gjennomføres i samsvar med framgangsmåtene angitt av den anmodende part, unntatt når de er uforenlige med den anmodede parts rett.
4. I tillegg til grunnene for avslag fastsatt i artikkel 25 nr. 4, kan den anmodede part avslå bistand dersom:
   a) anmodningen gjelder en straffbar handling som den anmodede part anser som en straffbar handling av politisk karakter eller knyttet til en straffbar handling av politisk karakter, eller
   b) den mener at gjennomføringen av en anmodning vil kunne krenke dens suverenitet, sikkerhet, ordre public eller andre vesentlige interesser.
5. Den anmodede part kan utsette iverksettelsen av skritt i henhold til en anmodning dersom dette kan skade etterforskningen eller den rettslige forfølgningen iverksatt av dens myndigheter.
6. Den anmodede part skal før den avslår eller utsetter sin hjelp og eventuelt etter å ha rådført seg med den anmodende part, vurdere om anmodningen kan etterkommes delvis eller på de vilkår den anser nødvendig.

7. Den anmodede part skal straks underrette den anmodende part om utfallet av gjennomføringen av en anmodning om hjelp. Dersom anmodningen avslås eller utsettes, skal grunnene til slikt avslag eller slik utsettelse oppgis. Den anmodede part skal også informere den anmodende part om eventuelle grunner som gjør det umulig å gjennomføre anmodningen eller som kan forsinke gjennomføringen betraktelig.
8. Den anmodende part kan be den anmodede part om fortrolig behandling av og innhold i en anmodning framsatt i henhold til dette kapittel, unntatt i den utstrekning det er nødvendig for å gjennomføre anmodningen. Dersom den anmodede part ikke kan etterkomme kravet om fortrolig behandling, skal den umiddelbart underrette den anmodende part, som så skal avgjøre om anmodningen likevel bør etterkommes.
9.
   a) Dersom saken haster, kan anmodninger om gjensidig hjelp eller meddelelser knyttet til slike anmodninger oversendes av de judisielle myndigheter i den anmodende part direkte til de tilsvarende myndigheter i den anmodede part. I slike tilfeller skal en kopi samtidig oversendes til den sentrale myn-

requested Party through the central authority of the requesting Party.

b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c) Where a request is made pursuant to subparagraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

dighet i den anmodede part via den sentrale myndighet i den anmodende part.

b) En anmodning eller en meddelelse etter dette nummer kan framsettes gjennom Den internasjonale kriminalpolitiorganisasjonen (Interpol).

c) Når en anmodning framsettes i henhold til bokstav a) og myndigheten ikke er kompetent til å behandle anmodningen, skal den henvise anmodningen til den kompetente nasjonale myndighet og underrette den anmodende part direkte om dette.

d) Anmodninger eller meddelelser framsatt i henhold til dette nummer som ikke innebærer tvangstiltak, kan oversendes av de kompetente myndigheter i den anmodende part direkte til de kompetente myndigheter i den anmodede part.

e) Hver part kan ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument, meddele Europarådets generalsekretær at anmodninger framsatt i henhold til dette nummer, av effektivitetshensyn, skal rettes til dens sentrale myndighet.

*Article 28 – Confidentiality and limitation on use*

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

   a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
   b) not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

*Artikkel 28 - Fortrolig behandling og begrensing i bruk*

1. Når det ikke foreligger noen avtale eller ordning om gjensidig hjelp basert på gjeldende felles eller gjensidig lovgivning mellom den anmodende og den anmodede part, skal bestemmelsene i denne artikkel gjelde. Bestemmelsene i denne artikkel får ikke anvendelse når en slik avtale, ordning eller lovgivning finnes, med mindre de berørte partene bestemmer å anvende i stedet hele eller deler av resten av denne artikkel.
2. Den anmodede part kan formidle opplysninger eller materiale som svar på en anmodning under den forutsetning av at slike opplysninger eller slikt materiale:
   a) behandles fortrolig når anmodningen om gjensidig hjelp ikke ville kunne etterkommes uten et slikt vilkår, eller
   b) ikke brukes til annen etterforskning eller rettslig forfølgning enn det som er angitt i anmodningen.
3. Dersom den anmodende part ikke kan oppfylle vilkåret nevnt i nr. 2, skal den omgående underrette den annen part, som så skal avgjøre om opplysningene likevel skal formidles. Når den anmodende part godtar vilkåret, skal den være bundet av det.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

### Section 2 – Specific provisions

#### Title 1 – Mutual assistance regarding provisional measures

*Article 29 – Expedited preservation of stored computer data*

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under paragraph 1 shall specify:
   a) the authority seeking the preservation;
   b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
   c) the stored computer data to be preserved and its relationship to the offence;
   d) any available information identifying the custodian of the stored computer data or the location of the computer system;
   e) the necessity of the preservation; and
   f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right

4. En part som formidler opplysninger eller materiale på et vilkår angitt i nr. 2, kan kreve at den annen part redegjør for bruken av slike opplysninger eller slikt materiale i forhold til det nevnte vilkår.

### Avsnitt 2 - Særlige bestemmelser

#### Del 1 - Gjensidig bistand i forbindelse med midlertidige tiltak

*Artikkel 29 - Hurtig sikring av lagrede, elektroniske data*

1. En part kan anmode en annen part om å beordre eller på annen måte sørge for hurtig sikring av elektroniske data som er lagret i et datasystem på territoriet til denne annen part, og for hvilke den anmodende part akter å framsette en anmodning om gjensidig bistand med sikte på ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data.
2. En anmodning om sikring framsatt etter nr. 1 skal angi:
   a) myndigheten som ber om sikring,
   b) den straffbare handling som er gjenstand for etterforskning og rettslig forfølgning samt en kort beskrivelse av de faktiske forhold i saken,
   c) de lagrede elektroniske data som skal sikres og deres sammenheng med den straffbare handlingen,
   d) alle tilgjengelige opplysninger for å kunne identifisere administrator av de elektroniske data eller stedet der datasystemet er plassert,
   e) nødvendigheten av sikring, og
   f) at parten akter å framsette en anmodning om gjensidig bistand med henblikk på ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av de lagrede elektroniske data.
3. Når den anmodede part mottar anmodningen fra den annen part, skal den treffe alle egnede tiltak for raskt å sikre de angitte data i samsvar med sin nasjonale rett. For å kunne etterkomme en slik anmodning skal dobbelt straffbart forhold ikke være et vilkår for å foreta slik sikring.
4. En part som stiller som vilkår at det foreligger dobbelt straffbart forhold for å etterkomme en anmodning om gjensidig bistand med sikte på ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data, kan for andre straffbare handlinger enn de som er fastslått i samsvar med artikkel 2 til 11 i denne

to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:
   a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

   b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

konvensjon, forbeholde seg retten til å avslå en anmodning om sikring etter denne artikkel dersom den har grunn til å tro at vilkåret om dobbelt straffbart forhold ikke kan oppfylles på avdekkingstidspunktet.

5. For øvrig kan en anmodning om sikring bare avslås dersom:
   a) anmodningen gjelder en straffbar handling som den anmodede part anser som en straffbar handling av politisk karakter eller knyttet til en straffbar handling av politisk karakter, eller
   b) den anmodede part mener at gjennomføringen av anmodningen kan krenke dens suverenitet, sikkerhet, ordre public eller andre vesentlige interesser.
6. Dersom den anmodede part mener at sikring ikke er noen garanti for at dataene vil være tilgjengelige i framtiden eller at det vil true den fortrolige behandlingen under den anmodende partens etterforskning eller på annen måte kan skade den, skal den straks gi underretning om dette til den anmodende part, som så skal avgjøre om anmodningen likevel bør gjennomføres.
7. All sikring utført for å etterkomme anmodningen omhandlet i nr. 1, skal vare minst 60 dager, slik at den anmodende part skal ha mulighet til å framsette en anmodning om ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data. Etter at en slik anmodning er mottatt, skal sikringen av data fortsette i påvente av en avgjørelse angående anmodningen.

*Article 30 – Expedited disclosure of preserved traffic data*

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if:
   a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

*Artikkel 30 - Hurtig utlevering av sikrede trafikkdata*

1. Dersom den anmodede part i løpet av gjennomføringen av en anmodning framsatt etter artikkel 29 om sikring av data knyttet til overføringen av en bestemt kommunikasjon oppdager at en tjenesteyter i en annen stat var involvert i overføringen av kommunikasjonen, skal den anmodede part raskt gi den anmodende part en tiltrekkelig mengde trafikkdata for å kunne identifisere vedkommende tjenesteyter og kommunikasjonsruten.

2. Utlevering av trafikkdata i henhold til nr. 1 kan bare avslås dersom:
   a) anmodningen gjelder en handling som den anmodede part anser som en straffbar handling av politisk karakter eller knyttet til en straffbar handling av politisk karakter, eller

b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

b) den anmodede part mener at gjennomføringen av anmodningen kan krenke dens suverenitet, sikkerhet, ordre public eller andre vesentlige interesser.

## Title 2 – Mutual assistance regarding investigative powers

*Article 31 – Mutual assistance regarding accessing of stored computer data*

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
3. The request shall be responded to on an expedited basis where:
   a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
   b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

## Del 2 Gjensidig hjelp med hensyn til etterforskningsmyndighet

*Artikkel 31 - Gjensidig hjelp for å få tilgang til lagrede, elektroniske data*

1. En part kan anmode en annen part om ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data som er lagret i et datasystem som befinner seg på den anmodede parts territorium, herunder data som er blitt sikret i henhold til artikkel 29.
2. Den anmodede part skal etterkomme anmodningen ved å anvende de internasjonale instrumentene, ordningene og lovgivningene nevnt i artikkel 23, og i samsvar med andre relevante bestemmelser i dette kapittel.
3. Anmodningen skal etterkommes omgående dersom:
   a) det er grunn til å tro at relevante data er spesielt utsatt for tap eller endring, eller
   b) instrumentene, ordningene og lovgivningene nevnt i nr. 2 inneholder annen bestemmelse om raskt samarbeid.

*Article 32 – Trans-border access to stored computer data with consent or where publicly available*

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

*Artikkel 32 - Grenseoverskridende tilgang til lagrede, elektroniske data, med samtykke eller når de er offentlig tilgjengelige*

En part kan uten å innhente tillatelse fra en annen part:

a) skaffe seg tilgang til offentlig tilgjengelige, lagrede data (åpne kilder), uansett hvor dataene befinner seg geografisk, eller
b) skaffe seg tilgang til eller motta via et datasystem på sitt territorium lagrede, elektroniske data som befinner seg i en annen stat, dersom parten innhenter lovlig og frivillig samtykke fra den person som har rettmessig myndighet til å avdekke data til parten via dette datasystemet.

*Article 33 – Mutual assistance regarding the real-time collection of traffic data*

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed

*Artikkel 33 - Gjensidig bistand i forbindelse med innhenting av trafikkdata i sanntid*

1. Partene skal yte hverandre gjensidig bistand i forbindelse med innhenting av trafikkdata i sanntid som er knyttet til bestemte kommunikasjoner på deres territorium, og som er overført ved hjelp av et datasystem. Med forbehold

by the conditions and procedures provided for under domestic law.
2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

for nr. 2 skal bistanden reguleres av de vilkår og prosedyrer som er fastsatt i nasjonal rett.
2. Hver part skal i det minste yte slik bistand i tilfeller der det i tilsvarende saker nasjonalt ville være adgang til innhente trafikkdata i sanntid.

*Article 34 – Mutual assistance regarding the interception of content data*

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

*Artikkel 34 - Gjensidig bistand i forbindelse med oppfanging av data knyttet til innhold*

Partene skal yte hverandre gjensidig bistand i forbindelse med innhenting eller registering i sanntid av data knyttet til innholdet i bestemte kommunikasjoner overført ved hjelp av et datasystem, i den utstrekning det gis adgang til det etter deres gjeldende avtaler og nasjonale rett.

**Title 3 – 24/7 Network**

*Article 35 – 24/7 Network*

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
   a) the provision of technical advice;
   b) the preservation of data pursuant to Articles 29 and 30;
   c) the collection of evidence, the provision of legal information, and locating of suspects.
2.
   a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
   b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

**Del 3-24/7 nettverk**

*Artikkel 35-24/7 nettverk*

1. Hver part skal utpeke et kontaktpunkt som er tilgjengelig 24 timer i døgnet, 7 dager i uken for å sikre omgående hjelp til etterforskning eller rettslig forfølgning av straffbare handlinger forbundet med datasystemer og data, eller for innhenting av elektroniske bevis for straffbare handlinger. Slik hjelp skal omfatte tilrettelegging for eller, dersom partens nasjonale rett og praksis tillater det, direkte:
   a) formidling av tekniske råd,
   b) sikring av data i henhold til artikkel 29 og 30, og
   c) innhenting av bevis, juridisk rådgivning og lokalisering av mistenkte.
2.
   a) En parts kontaktpunkt skal ha mulighet til å kommunisere med en annen parts kontaktpunkt etter en hasteprosedyre.
   b) Dersom kontaktpunktet utpekt av en part ikke er en del av denne partens myndighet eller myndigheter som har ansvaret for internasjonal gjensidig bistand eller utlevering, skal kontaktpunktet påse at det er i stand til å samordne sitt arbeid med slik myndighet eller slike myndigheter etter en hasteprosedyre.
3. Hver part skal sørge for å ha tilgjengelig personell med nødvendig opplæring og utstyr for å lette nettverkets arbeid.

## Chapter IV – Final provisions

*Article 36 – Signature and entry into force*

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

*Article 37 – Accession to the Convention*

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

*Article 38 – Territorial application*

1. Any State may, at the time of signature or when depositing its instrument of ratification, accep-

## Kapittel IV - Sluttbestemmelser

*Artikkel 36 - Undertegning og ikrafttredelse*

1. Denne konvensjon skal være åpen for undertegning av Europarådets medlemsstater og ikke-medlemsstater som har deltatt i utarbeidelsen av konvensjonen.
2. Denne konvensjon skal ratifiseres, godtas eller godkjennes. Ratifikasjons-, godtakelses- eller godkjenningsdokumentene skal deponeres hos Europarådets generalsekretær.
3. Denne konvensjon skal tre i kraft den første dagen i måneden etter utløpet av et tidsrom på tre måneder regnet fra den dag fem stater, hvorav minst tre medlemsstater i Europarådet, har gitt sitt samtykke til å være bundet av konvensjonen i samsvar med bestemmelsene i nr. 1 og 2.
4. For en signatarstat som på et senere tidspunkt gir sitt samtykke til å være bundet av konvensjonen, skal konvensjonen tre i kraft den første dagen i måneden etter utløpet av et tidsrom på tre måneder regnet fra den dag den har gitt sitt samtykke til å være bundet av konvensjonen i samsvar med bestemmelsene i nr. 1 og 2.

*Artikkel 37 - Tiltredelse*

1. Etter at denne konvensjon er trådt i kraft, kan Europarådets ministerkomité etter å ha rådført seg med konvensjonsstatene og innhentet deres enstemmige samtykke, invitere en stat som ikke er medlem av Europarådet og som ikke har deltatt i utarbeidelsen av konvensjonen, til å tiltre denne konvensjon. Beslutningen skal treffes med det flertall som er fastsatt i artikkel 20 bokstav d) i Europarådets vedtekter, og ved enstemmighet blant representantene for de konvensjonsstater som har rett til å delta i ministerkomiteen.
2. For en stat som tiltrer konvensjonen etter nr. 1 ovenfor, skal den tre i kraft den første dag i måneden som følger etter utløpet av et tidsrom på tre måneder regnet fra den dag tiltredelsesdokumentet er deponert hos Europarådets generalsekretær.

*Artikkel 38 - Territorial anvendelse*

1. En stat kan ved undertegning eller deponering av sitt ratifikasjons-, godtakelses-, godkjen-

tance, approval or accession, specify the territory or territories to which this Convention shall apply.
2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

nings- eller tiltredelsesdokument nærmere angi det eller de territorier som denne konvensjon får anvendelse på.
2. En stat kan på ethvert senere tidspunkt ved erklæring rettet til Europarådets generalsekretær utvide denne konvensjonens anvendelse til ethvert annet territorium som angis i erklæringen. For slikt territorium skal konvensjonen tre i kraft den første dag i måneden som følger etter utløpet av et tidsrom på tre måneder regnet fra den dag Generalsekretæren mottok slik erklæring.
3. En erklæring avgitt i henhold til de to foregående numre kan trekkes tilbake for et territorium angitt i slik erklæring ved underretning til Europarådets generalsekretær. Tilbaketrekkingen får virkning den første dagen i måneden som følger etter utløpet av et tidsrom på tre måneder regnet fra den dag Generalsekretæren mottok slik underretning.

*Article 39 – Effects of the Convention*

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
   - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
   - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
   - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).
2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

*Artikkel 39 - Konvensjonens virkninger*

1. Formålet med denne konvensjon er å utfylle eksisterende multilaterale eller bilaterale avtaler eller ordninger som får anvendelse mellom partene, herunder bestemmelsene i:
   - Den europeiske konvensjon om utlevering åpnet for undertegning i Paris 13. desember 1957 (ETS nr. 24),
   - Den europeiske konvensjon om gjensidig bistand i straffesaker åpnet for undertegning i Strasbourg 20. april 1959 (ETS nr. 30),
   - Tilleggsprotokoll til Den europeiske konvensjon om gjensidig bistand i straffesaker åpnet for undertegning i Strasbourg 17. mars 1978 (ETS nr. 99).
2. Dersom to eller flere parter allerede har inngått en avtale eller en traktat om spørsmål omhandlet i denne konvensjon eller på annen måte har etablert sine forbindelser i slike spørsmål, eller vil gjøre det i framtiden, skal de også ha rett til å anvende slik avtale eller traktat eller regulere slike forbindelser i samsvar med disse. Dersom partene imidlertid etablerer forbindelser som gjelder spørsmål omhandlet i denne konvensjon på annen måte enn det som er fastsatt i denne konvensjon, skal dette gjøres på en måte som ikke er uforenlig med denne konvensjonens mål og prinsipper.
3. Ingen bestemmelse i denne konvensjon skal berøre en parts øvrige rettigheter, restriksjoner, forpliktelser og ansvar.

*Article 40 – Declarations*

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

*Article 41 – Federal clause*

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

*Article 42 – Reservations*

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

*Article 43 – Status and withdrawal of reservations*

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification ad-

*Artikkel 40 - Erklæringer*

En stat kan ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings eller tiltredelsesdokument og ved skriftlig underretning til Europarådets generalsekretær erklære at den benytter seg av adgangen til å stille tilleggsvilkårene fastsatt i artikkel 2, artikkel 3, artikkel 6 nr. 1 b), artikkel 7, artikkel 9 nr. 3 og artikkel 27 nr. 9 e).

*Artikkel 41 - Forbundsstatsklausul*

1. En forbundsstat kan forbeholde seg retten til å påta seg forpliktelser etter kapittel II i denne konvensjon i overensstemmelse med dens grunnleggende prinsipper som regulerer forholdet mellom dens sentrale regjering og delstatene eller andre liknende territoriale enheter, forutsatt at den fremdeles er i stand til å samarbeide etter kapittel III.
2. Når en forbundsstat framsetter et forbehold i henhold til nr. 1, kan den ikke anvende vilkårene i et slikt forbehold til å utelukke eller i vesentlig grad innskrenke sine forpliktelser til å sørge for tiltak fastsatt i kapittel II. Den skal i hovedsak sørge for å ha omfattende og effektive midler til rådighet for å håndheve de nevnte tiltakene.
3. Med hensyn til bestemmelser i denne konvensjon hvis anvendelse hører inn under jurisdiksjonen til en delstat eller liknende territorial enhet som etter forbundsstatens konstitusjonelle system ikke er forpliktet til å treffe lovtiltak, skal den føderale regjeringen informere de kompetente myndigheter i disse statene om de nevnte bestemmelser og gi sin positive uttalelse, samt oppmuntre dem til å treffe hensiktsmessige tiltak for å iverksette dem.

*Artikkel 42 - Forbehold*

En stat kan ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument, erklære ved skriftlig underretning til Europarådets generalsekretær om at den ønsker å ta ett eller flere av forbeholdene fastsatt i artikkel 4 nr. 2, artikkel 6 nr. 3, artikkel 9 nr. 4, artikkel 10 nr. 3, artikkel 11 nr. 3, artikkel 14 nr. 3, artikkel 22 nr. 2, artikkel 29 nr. 4 og artikkel 41 nr. 1. Det kan ikke tas andre forbehold.

*Artikkel 43 - Status og tilbaketrekking av forbehold*

1. En part som har tatt et forbehold i samsvar med artikkel 42, kan helt eller delvis trekke forbeholdet tilbake ved underretning til Europarå-

dressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

dets generalsekretær. Tilbaketrekkingen får virkning den dag generalsekretæren mottar underretningen. Dersom det i underretningen er oppgitt at tilbaketrekkingen av et forbehold skal få virkning på en angitt dato, og denne dato inntreffer senere enn den dag generalsekretæren mottar underretningen, skal underretningen tre i kraft på en slik senere dato.

2. En part som har tatt et forbehold i samsvar med artikkel 42, skal trekke forbeholdet tilbake helt eller delvis så snart omstendighetene tillater det.
3. Europarådets generalsekretær kan regelmessig rette en forespørsel til partene som har tatt ett eller flere forbehold i samsvar med artikkel 42 om utsiktene for tilbaketrekking av disse forbehold.

*Article 44 – Amendments*

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

*Artikkel 44 - Endringer*

1. Enhver part kan foreslå endringer i denne konvensjon, og Europarådets generalsekretær skal oversende dem til Europarådets medlemsstater, til enhver ikke-medlemsstat som har deltatt i utarbeidelsen av denne konvensjon, samt til enhver stat som har tiltrådt eller som er blitt invitert til å tiltre konvensjonen i samsvar med bestemmelsene i artikkel 37.

2. Enhver endring som foreslås av en part, skal oversendes Europarådets komité for kriminalspørsmål (CDPC), som skal legge fram en uttalelse for Ministerkomiteen om endringsforslaget.
3. Ministerkomiteen skal behandle endringsforslaget og uttalelsen fra CDPC, og kan vedta endringen etter å ha rådført seg med ikke-medlemsstater som er part i denne konvensjon.

4. Den endringstekst som vedtas av Ministerkomiteen i samsvar med nr. 3 i denne artikkel, skal oversendes partene for godtakelse.

5. En endring som vedtas i samsvar med nr. 3 i denne artikkel, skal tre i kraft den trettiende dag etter at alle parter har underrettet generalsekretæren om at de godtar endringen.

*Article 45 – Settlement of disputes*

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

*Artikkel 45 - Tvisteløsning*

1. Europarådets komité for kriminalspørsmål (CDPC) skal holdes underrettet om tolkningen og anvendelsen av denne konvensjon.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

2. Dersom det oppstår en tvist mellom partene om tolkningen eller anvendelsen av denne konvensjon, skal de søke å løse tvisten ved forhandling eller andre fredelige midler etter eget valg, herunder henvisning av tvisten til CDPC, til en voldgiftsrett hvis avgjørelser skal være bindende for partene, eller til Den internasjonale domstol, etter overenskomst mellom de berørte parter.

*Article 46 – Consultations of the Parties*

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:
   a) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
   b) the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
   c) consideration of possible supplementation or amendment of the Convention.
2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.
3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

*Artikkel 46 - Konsultasjoner mellom partene*

1. Partene skal etter behov regelmessig konsultere hverandre for å tilrettelegge for:
   a) effektiv bruk og gjennomføring av denne konvensjon, herunder påpeke problemer i denne forbindelse, samt følgene av en erklæring avgitt eller et forbehold framsatt i henhold til denne konvensjon,
   b) utveksling av opplysninger om rettslig, politisk eller teknologisk utvikling av betydning for datakriminalitet og innhenting av elektroniske bevis,
   c) vurdering av eventuelle tilføyelser eller endringer i konvensjonen.
2. Europarådets komité for kriminalspørsmål (CDPC) skal holdes løpende informert om resultatene av konsultasjoner omhandlet i nr. 1.

3. CDPC skal ved behov tilrettelegge for konsultasjoner omhandlet i nr. 1 og treffe de nødvendige tiltak for å bistå partene i deres anstrengelser for å utfylle eller endre konvensjonen. Senest tre år etter at denne konvensjon er trådt i kraft skal Europarådets komité for kriminalspørsmål (CDPC) i samarbeid med partene foreta en gjennomgang av alle bestemmelsene i konvensjonen og om nødvendig anbefale hensiktsmessige endringer.

4. Utgifter som påløper i forbindelse med gjennomføringen av bestemmelsene i nr. 1, skal, med mindre Europarådet påtar seg slike utgifter, bæres av partene på den måten de bestemmer.
5. Europarådets sekretariat skal bistå partene i forbindelse med utføringen av deres oppgaver i henhold til denne artikkel.

*Article 47 – Denunciation*

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

*Artikkel 47 - Oppsigelse*

1. En part kan til enhver tid si opp denne konvensjon ved underretning til Europarådets generalsekretær.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

2. Slik oppsigelse får virkning den første dag i måneden etter utløpet av et tidsrom på tre måneder regnet fra den dag Generalsekretæren mottok underretningen.

*Article 48 – Notification*

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a) any signature;
b) the deposit of any instrument of ratification, acceptance, approval or accession;
c) any date of entry into force of this Convention in accordance with Articles 36 and 37;
d) any declaration made under Article 40 or reservation made in accordance with Article 42;
e) any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

*Artikkel 48 - Underretninger*

Europarådets generalsekretær skal underrette Europarådets medlemsstater, de ikke-medlemsstatene som har deltatt i utarbeidelsen av denne konvensjon, samt enhver stat som har tiltrådt eller som er blitt invitert til å tiltre konvensjonen, om:

a) enhver undertegning
b) deponering av ethvert ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument,
c) enhver ikrafttredelsesdato for denne konvensjon i samsvar med artikkel 36 og 37,
d) enhver erklæring avgitt i henhold til artikkel 40 eller forbehold tatt i samsvar med artikkel 42,
e) enhver annen handling, underretning eller meddelelse som gjelder denne konvensjon.

Til bekreftelse på dette har de undertegnede, som har fått behørig fullmakt til det, undertegnet denne konvensjon.

Utferdiget i Budapest, den 23. november 2001 på engelsk og fransk, med samme gyldighet for begge tekster, i ett eksemplar som skal deponeres i Europarådets arkiver. Europarådets generalsekretær skal oversende bekreftede kopier til hver medlemsstat i Europarådet, til de ikke-medlemsstater som har deltatt i utarbeidelsen av denne konvensjon, og til enhver stat som er blitt invitert til å tiltre konvensjonen.

**Vedlegg 2**

# Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

## Chapter I – Common provisions

### *Article 1 – Purpose*

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as «the Convention»), as regards

the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

*Article 2 – Definition*

1. For the purposes of this Protocol:
   «racist and xenophobic material» means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.
2. The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

## Chapter II – Measures to be taken at national level

*Article 3 – Dissemination of racist and xenophobic material through computer systems*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.
3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

*Article 4 – Racist and xenophobic motivated threat*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

*Article 5 – Racist and xenophobic motivated insult*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.
2. A Party may either:
   a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or
   b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

*Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity*

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:
   distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.
2. A Party may either
   a) require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite

hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

*Article 7 – Aiding and abetting*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

## Chapter III – Relations between the Convention and this Protocol

*Article 8 – Relations between the Convention and this Protocol*

1. Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, mutatis mutandis, to this Protocol.
2. The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

## Chapter IV – Final provisions

*Article 9 – Expression of consent to be bound*

1. This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:
   a) signature without reservation as to ratification, acceptance or approval; or
   b) subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.
2. A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.
3. The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

*Article 10 – Entry into force*

1. This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.
2. In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

*Article 11 – Accession*

1. After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.
2. Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

*Article 12 – Reservations and declarations*

1. Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.
2. By a written notification addressed to the Secretary General of the Council of Europe, any Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.
3. By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it

avails itself of the possibility of requiring additional elements as provided for in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

*Article 13 – Status and withdrawal of reservations*

1. A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
2. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

*Article 14 – Territorial application*

1. Any Party may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Protocol shall apply.
2. Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

*Article 15 – Denunciation*

1. Any Party may, at any time, denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

*Article 16 – Notification*

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol of:

a) any signature;
b) the deposit of any instrument of ratification, acceptance, approval or accession;
c) any date of entry into force of this Protocol in accordance with its Articles 9, 10 and 11;
d) any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 28th day of January 2003, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Protocol, and to any State invited to accede to it.