Innst. O. nr. 53

(2004-2005)

Innstilling til Odelstinget fra justiskomiteen

Ot.prp. nr. 40 (2004-2005)

Innstilling fra justiskomiteen om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)

Til Odelstinget

1. SAMMENDRAG

1.1 Proposisjonens hovedinnhold

I proposisjonen fremmer departementet forslag om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi, og om endringer i straffeloven og straffeprosessloven for å gjennomføre de forpliktelser som Norge vil påta seg ved ratifikasjonen.

For det første foreslår departementet et nytt straffebud som forbyr forskjellige former for urettmessig befatning med passord og andre tilgangsdata, og med dataprogrammer og andre innretninger som er særlig egnet til å begå straffbare handlinger rettet mot data eller datasystemer.

For det annet foreslår departementet regler om midlertidig sikring av elektronisk lagrete data. Det tredje forslaget innebærer at politiet, under ransaking av et datasystem, vil kunne pålegge enhver å gi de opplysninger som er nødvendige for å få tilgang til datasystemet.

1.2 Konvensjonens straffebestemmelser

Norsk strafferett er i det alt vesentlige i samsvar med de krav konvensjonen stiller. Datakrimutvalget la således til grunn at det ikke var behov for andre lovendringer enn dem som artikkel 6 gjør nødvendig, noe høringsinstansene har sluttet seg til. Departementet er enig i dette.

1.2.1 Datainnbrudd

Konvensjonen artikkel 2 gjelder datainnbrudd. Bestemmelsen pålegger konvensjonsstatene å sette straff for den som rettsstridig skaffer seg tilgang til hele eller deler av et datasystem, uavhengig av om vedkommende har gjort seg kjent med innholdet av de data som datainnbruddet har gitt tilgang til.

Datainnbrudd rammes av straffeloven § 145 annet ledd. Bestemmelsen rammer bare den som "ved å bryte en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data eller programutrustning". Det er ikke et vilkår for straff at gjerningspersonen har gjort seg kjent med dataene eller programutrustningen. Etter bestemmelsen er det tilstrekkelig at hun eller han har skaffet seg adgang til dem.

Utvalget drøfter forholdet mellom artikkel 2 og straffeloven § 145 annet ledd og går inn for å endre bestemmelsen slik at overtredelser kan straffes med fengsel inntil 6 måneder eller bøter eller begge deler.

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. På bakgrunn av særlig Økokrims høringsuttalelse 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, er imidlertid en oppgave av en slik art at det er naturlig å la den gå inn i Datakrimutvalgets videre arbeid. Spørsmålet blir da om det er et mer akutt behov for å følge opp forslaget i høringsbrevet (å fjerne beskyttelsesvilkåret) allerede nå, eller om også dette

mer avgrensede spørsmålet best kan følges opp i Datakrimutvalgets andre delutredning.

Selv om de fleste høringsinstansene som har uttalt seg om spørsmålet går inn for å fjerne vilkåret om beskyttelsesbrudd, underbygger ikke høringen at det er noe påtrengende behov for å foreslå en slik lovendring nå. Departementet foreslår derfor ikke nå å fjerne dette vilkåret i straffeloven § 145 annet ledd. Dette innebærer i tilfelle at det må avgis en erklæring i samsvar med artikkel 40.

Departementet er enig med utvalget og Politidirektoratet i at straffen for overtredelsen av bestemmelsen bør skjerpes noe, og tiltrer utvalgets forslag. Dette vil sikre at det kan brukes straffeprosessuelle tvangsmidler i den utstrekning konvensjonen krever.

1.2.2 Ulovlig spredning av tilgangsdata - artikkel 6

Artikkel 6 gjelder besittelse og spredning av visse dataprogrammer, tilgangsdata mv., og pålegger konvensjonsstatene å sette straff for produksjon, salg, kjøp, import, distribusjon og andre former for spredning av dataprogrammer og andre innretninger som er utformet eller tilpasset for å kunne begå straffbare handlinger som nevnt i artikkel 2 til 5. I underpunkt ii rammes tilsvarende former for befatning med passord, tilgangskoder og lignende data som er egnet til å gi tilgang til hele eller deler av et datasystem.

I norsk lovgivning finnes det ingen straffebestemmelse som fullt ut dekker de handlingene som er beskrevet i artikkel 6, og Datakrimutvalget la til grunn at artikkel 6 gjør det nødvendig med lovendringer.

Etter departementets syn kan det ikke være tvilsomt at artikkel 6 gjør det nødvendig med lovendringer. Dette gjelder selv om reservasjonsadgangen i artikkel 6 nr. 3 benyttes.

BØR RESERVASJONSADGANGEN BENYTTES?

I NOU 2003:27 blir spørsmålet om og i tilfelle i hvilken utstrekning Norge bør benytte reservasjonsadgangen i artikkel 6 nr. 3 drøftet. Utvalget mener at Norge bør reservere seg mot å oppstille straffansvar for besittelse av visse dataprogrammer. Utvalget går heller ikke inn for å kriminalisere det å gjøre slike innretninger tilgjengelige for andre.

Artikkel 6 innebærer en forpliktelse til å kriminalisere forberedelseshandlinger. Det kreves en tungtveiende begrunnelse for å sette straff for forberedelseshandlinger. At grensen mellom forberedelse til samfunnsskadelige handlinger og forberedelser til helt uskyldige handlinger i stor grad beror på sinnelaget til personen som begår dem, taler generelt med tyngde imot at slike handlinger skal kriminaliseres. Dette synspunktet får imidlertid mer begrenset bærekraft når den aktuelle forberedelseshandlingen i større utstrekning bidrar til å kaste lys over gjerningspersonens forsett. Hackerverktøy mv. er særlig egnet til å begå straffbare handlinger. Et straffebud som retter seg mot det å besitte slike innretninger, vil dermed være mer treffsikkert enn et straffebud som retter seg mot mer dagligdagse handlinger.

Etter departementets syn taler både det betydelige skadepotensialet, hensynet til tilliten til elektronisk kommunikasjon og den tilsynelatende lave oppdagelsesrisikoen for at det bør være straffbart å besitte hackerverktøy og andre tilsvarende innretninger. Det vil også lette det internasjonale samarbeidet i saker som gjelder datakriminalitet. Departementet har på denne bakgrunn kommet til at det bør settes straff for besittelse av passord og hackerverktøy mv.

Departementet går så over til å drøfte spørsmålet om det bør settes straff for å gjøre slike innretninger tilgjengelige for andre. I Datakrimutvalgets utredning ble det foreslått at heller ikke slike handlinger kriminaliseres. Etter departementets syn har de momentene som det er vist til i drøftelsen ovenfor, minst like stor gjennomslagskraft i spredningstilfellene. Også spredning bør derfor kriminaliseres. Siden slike handlinger ofte er straffbare allerede etter reglene om forsøk og medvirkning, vil en slik utvidelse innebære en forholdsvis beskjeden nykriminalisering.

NÆRMERE OM UTFORMINGEN AV BESTEMMELSEN

I utvalgets utredning foreslås det at artikkel 6 nr. 1 bokstav a (ii) blir gjennomført i en ny straffebestemmelse, og at bestemmelsens objektive gjerningsinnhold utformes slik at den "ikke begrenses til å gjelde passord, men må gjelde alle former for data som kan gi tilgang til hele eller deler av et datasystem".

Departementet er enig med utvalget i at artikkel 6 bør gjennomføres i en ny straffebestemmelse, som foreslås som ny § 145b i straffeloven. Det finnes ingen bestemmelse som fra før rammer tilsvarende forhold som det konvensjonen retter seg mot.

Når det gjelder bestemmelsens objektive gjerningsinnhold, omfatter antakelig konvensjonen enhver logisk eller fysisk innretning som er særlig egnet ved overtredelse av artikkel 2 til 5. For å sikre at Norge lojalt oppfyller sine folkerettslige forpliktelser er lovutkastet utformet i samsvar med det. Departementet er enig med utvalget i at bestemmelsen må utformes slik at den gjelder alle former for data som kan gi tilgang til hele eller deler av et datasystem.

Vedrørende hvilke befatningsformer som skal rammes, er det etter departementets syn tilstrekkelig om den norske gjennomføringsbestemmelsen rammer befatningsformene fremstille, anskaffe, besitte eller gjøre tilgjengelig for andre. Straffansvar kan

bare komme på tale der den aktuelle befatningsformen er uberettiget.

Når det gjelder skyldkravet, blir spørsmålet om det bør kreves at gjerningspersonen har til hensikt å begå straffbare handlinger, slik konvensjonen legger opp til, eller om det bør være tilstrekkelig med alminnelig forsett. Departementet er enig med utvalget i at også rent forsettlige overtredelser av bestemmelsen er straffverdige. Det bør derfor ikke kreves at handlingen er begått med en bestemt hensikt.

Datakrimutvalget foreslo å sette strafferammen til bøter eller fengsel i 6 måneder eller begge deler. For grove tilfeller foreslo utvalget en strafferamme på fengsel i 2 år. Departementet slutter seg til utvalgets vurderinger på dette punkt.

Når det gjelder bestemmelsens stedlige virkeområde, er departementet enig med utvalget i at bestemmelsen bør føyes til straffeloven § 12 nr. 3. Tilføyelsen vil innebære at utkastet til ny § 145b vil kunne ramme handlinger som er begått i utlandet av norske statsborgere eller andre som er hjemmehørende i Norge.

1.3 Konvensjonens bestemmelser om straffeprosessuelle spørsmål

Norsk straffeprosess er på de fleste punkter i samsvar med de krav konvensjonen stiller. Datakrimutvalget la således til grunn at det ikke var behov for andre lovendringer enn dem som artikkel 16, 17 nr. 1 bokstav b og 19 nr. 4 gjør nødvendig, noe høringsinstansene har sluttet seg til. Departementet er enig i dette.

1.3.1 Midlertidig sikring av lagrete data (sikringspålegg)

KONVENSJONSFORPLIKTELSEN

Artikkel 16 gjelder midlertidig sikring av elektronisk lagrede data, og gir regler om midlertidig sikring av data som antas å ha betydning som bevis i en straffesak. Størst praktisk betydning får bestemmelsen for data som foreløpig ikke kan kreves utlevert. Bestemmelsen omfatter alle former for data som er elektronisk lagret, både trafikkdata og innholdsdata. Et sikringspålegg kan imidlertid bare rette seg mot data som er lagret på sikringstidspunktet. Data som er under overføring faller utenfor bestemmelsens virkeområde. Et sikringspålegg skal ikke gjelde for et lengre tidsrom enn nødvendig, og uansett ikke for mer enn 90 dager om gangen. Besluttes et sikringspålegg etter anmodning fra en fremmed stat, følger det av artikkel 29 at dataene skal sikres i minst 60 dager.

Artikkel 17 gir særregler om trafikkdata, og innebærer at trafikkdata må kunne sikres midlertidig også i de tilfeller hvor flere tjenestetilbydere er involvert i en kommunikasjonsoverføring. Siden trafikkdata ofte blir slettet etter relativt kort tid, kan det føre til at viktige bevis går tapt. Artikkel 17 åpner derfor for at myndighetene umiddelbart skal gis tilgang til trafikkdata i den utstrekning det er nødvendig for å avklare om andre tjenestetilbydere har vært involvert.

ER DET BEHOV FOR LOVENDRINGER?

Datakrimutvalget la til grunn i sin utredning at straffeprosessloven § 216 ikke fullt ut oppfyller forpliktelsene i artikkel 16 og 17 nr. 1 bokstav a, og at det er klart at konvensjonens bestemmelser om midlertidig sikring av data gjør det nødvendig med lovendringer.

Derimot var utvalget mer i tvil om det er nødvendig å endre straffeprosessloven § 210 for å oppfylle forpliktelsen i artikkel 17 nr. 1 bokstav b om utlevering av trafikkdata. Adgangen til å gi utleveringspålegg overfor tjenestetilbydere er betinget av at Post- og teletilsynet gir fritak fra taushetsplikten etter ekomloven. Skal denne ordningen videreføres, vil tilsynet i tilfelle måtte gi fritak i alle de saker som faller innenfor artikkel 17 nr. 1 bokstav b, og det vil innbære at tilsynsfunksjonen blir uten realitet. Etter utvalgets syn er det lite å vinne på en slik ordning, og det foreslo i stedet en egen bestemmelse om utlevering av visse trafikkdata.

Etter departementets syn er det ikke tvilsomt at artikkel 16 og 17 nr. 1 bokstav a gjør det nødvendig med lovendringer i norsk rett. Departementet er videre enig med utvalget i at det bør gis en særskilt bestemmelse om utlevering av trafikkdata som nevnt i artikkel 17 nr. 1 bokstav b.

NÆRMERE OM UTFORMINGEN AV BESTEMMELSEN

Utvalgets forslag

I utredningen foreslås det at artikkel 16 og 17 bør gjennomføres i en ny bestemmelse i straffeprosessloven. Utvalget drøfter hvilke former for data som bestemmelsen skal omfatte, og konkluderer med at alle former for data, inkludert e-post og andre former for innholdsdata, bør med. Utvalget understreker at mistanken må bygge på objektive holdepunkter. Noe kvalifisert mistankekrav går utvalget imidlertid ikke inn for.

Et særlig spørsmål er om adgangen til å utferdige sikringspålegg bør variere avhengig av om pålegget retter seg mot innholdsdata eller trafikkdata. Utvalgets flertall mener at det bør trekkes et skille mellom trafikkdata og andre former for data. Etter flertallets syn bør sikring av andre data enn trafikkdata bare kunne skje ved mistanke om en straffbar handling med en høyere strafferamme enn fengsel i 6 måneder. Utvalgets mindretall foreslår at strafferammekravet bare bør knyttes til midlertidig sikring av e-post.

Utvalget går inn for at den som opplysningene knytter seg til, skal gis underretning om sikringspålegget. Etter utvalgets syn bør en mistenkt ha krav på

underretning fra det tidspunkt han får status som siktet i saken.

Når det gjelder bestemmelsen om utlevering av visse trafikkdata etter artikkel 17 nr. 1 bokstav b, foreslår utvalgets flertall at forpliktelsen gjennomføres slik at politiet etter en særskilt bestemmelse skal få tilgang til opplysninger som er nødvendige for å avdekke hvor de aktuelle dataene kom fra eller ble sendt til.

DEPARTEMENTETS SYN

Etter departementets syn må de nye reglene om sikringspålegg utformes i lys av reglene om beslag. Slik artikkel 16 nr. 1 er formulert, legger departementet til grunn at bestemmelsen må omfatte alle former for data, inkludert e-post og andre kategorier av innholdsdata.

I spørsmålet om hvilke vilkår et sikringspålegg bør gjøres betinget av, bør det etter departementets oppfatning i utgangspunktet være tilstrekkelig at dataene kan ha betydning som bevis. Men departementet går inn for at pålegg til en tjenestetilbyder om å sikre e-post og eventuelle vedlegg bør være betinget av at det er grunn til å tro at det er begått en straffbar handling. En slik løsning er best i samsvar med reglene om beslag av brev og andre postsendinger i straffeprosessloven.

Konvensjonen angir ikke på hvilken måte sikringen skal skje. Departementet er enig med utvalget i at bestemmelsen bør utformes teknologinøytralt, og at det derfor ikke bør sies noe bestemt i loven om hvordan dataene skal sikres.

Departementet er enig med utvalget i at kompetansen til å beslutte midlertidig sikring av data bør ligge hos påtalemyndigheten.

Departementet er enig med utvalget i at en mistenkt bør ha krav på underretning fra det tidspunkt han får status som siktet i saken, men bare dersom sikringspålegget gjelder data som den siktede selv har lovlig tilgang til. Etter departementets syn taler de beste grunner for at også den som er utenfor mistanke, bør få underretning i samme utstrekning som den mistenkte. En slik løsning er best i samsvar med straffeprosesslovens system ved bruk av andre tvangsmidler.

Det siste spørsmålet er om en beslutning om bruk av sikringspålegg bør kunne gjøres til gjenstand for rettslig prøving. Utvalget har foreslått at det bør være adgang til rettslig overprøving, og departementet er enig i det.

SIKRINGSPÅLEGG SOM LEDD I INTERNASJONALT SAMARBEID I STRAFFESAKER

Konvensjonen artikkel 29 pålegger statspartene å etterkomme en anmodning om å utferdige et sikringspålegg selv om forholdet ikke er straffbart i staten som anmodes om å yte bistand. Artikkel 29 nr. 4 gir imidlertid stater som Norge, som har dobbel straffbarhet som et vilkår for å yte rettshjelp, mulighet til å reservere seg mot forpliktelsen til å utferdige sikringspålegg i saker som gjelder forhold som ikke er straffbare i Norge. Utvalget går inn for at Norge benytter seg av denne muligheten.

Også departementet har kommet til at kravet om dobbel straffbarhet bør opprettholdes for anmodninger om sikringspålegg. Prinsippet om dobbel straffbarhet sikrer at Norge ikke yter rettshjelp i saker som sett fra et norsk ståsted ikke bør gi grunnlag for bruk av tvangsmidler.

1.3.2 Opplysningsplikt under ransaking

Artikkel 19 nr. 4 gjelder opplysningsplikt under ransaking og pålegger konvensjonsstatene å gi regler om opplysningsplikt under ransaking av et datasystem. I norsk rett finnes det ingen generell regel om opplysningsplikt av den type som artikkel 19 forutsetter. For å gjennomføre konvensjonsforpliktelsen er det derfor nødvendig med en ny lovbestemmelse.

Utvalget mener at artikkel 19 nr. 4 gjør det påkrevd å endre straffeprosessloven. Utvalget fremhever samtidig at pålegg om å gi opplysninger i forbindelse med en ransaking kan tenkes å komme i konflikt med vernet mot selvinkriminering På denne bakgrunn foreslår utvalget at opplysningsplikten bare kan pålegges den som plikter å vitne i saken. Når det gjelder selve utformingen av bestemmelsen, går utvalget inn for at opplysningsplikten ikke bør gis et større omfang enn konvensjonen artikkel 19 nr. 4 krever.

Departementet vil peke på at konvensjonsforpliktelsen etter artikkel 19 nr. 4 bare omfatter opplysninger som trengs for å gi tilgang til det datasystemet som skal ransakes. Slike opplysninger vil i seg selv neppe være egnet til å utsette angiveren for straff. Allerede av den grunn anser departementet det lite sannsynlig at vernet mot selvinkriminering vil innebære noen begrensning for å kreve opplysninger etter artikkel 19 nr. 4.

Departementet ser på denne bakgrunn ingen grunn til å begrense rekkevidden av opplysningsplikten om tilgang til datasystemer slik det går frem av konvensjonens artikkel 19 nr. 4. Departementet er på den annen side enig med utvalget i at opplysningsplikten ikke bør gis et større omfang enn konvensjonen krever.

1.4 Bør Norge ratifisere konvensjonen?

Departementet er ikke i tvil om at konvensjonen vil bidra til å styrke det internasjonale samarbeidet i saker av denne type. Det er viktig at Norge sammen med de andre medlemsstatene følger opp og slutter seg til konvensjonen.

Departementet er enig med utvalget i at Norge ikke bør åpne for innhenting av trafikkdata i sanntid i mindre alvorlige straffesaker, jf. artikkel 20. Det bør dessuten avgis erklæringer i tilknytning til artikkel 2 og 29, slik utvalget foreslår. I tillegg må Norge avgi erklæringer i tilknytning til artikkel 24 og 27.

På denne bakgrunn ber departementet om Stortingets samtykke til ratifikasjon av konvensjonen med den reservasjon og de erklæringer som nevnt ovenfor.

1.5 Økonomiske og administrative konsekvenser

De foreslåtte lovendringene vil neppe få større økonomiske eller administrative konsekvenser.

2. KOMITEENS MERKNADER

Komiteen, medlemmene fra Arbeiderpartiet, Anne Helen Rui, Ola Røtvei og Knut Storberget, fra Høyre, lederen Trond Helleland, Linda Cathrine Hofstad og Ingjerd Schou, fra Fremskrittspartiet, Jan Arild Ellingsen og André Kvakkestad, fra Kristelig Folkeparti, Einar Holstad og Finn Kristian Marthinsen, og fra Sosialistisk Venstreparti, Inga Marte Thorkildsen, viser til den fremlagte proposisjonen om lovtiltak mot datakriminalitet.

Komiteen støtter intensjonen i forslaget fra Regjeringen i Ot.prp. nr 40 (2004-2005) om bekjempelse av kriminalitet som er knyttet til informasjons- og kommunikasjonsteknologi. Dette er et fagfelt hvor den teknologiske utviklingen skjer meget hurtig, noe som gjør det utfordrende å ha et lovverk som til enhver tid er tilpasset teknologien. Komiteen er derfor positiv til de fleste av de forslag som her fremsettes.

Komiteen registrerer at også andre land støtter opp om dette arbeidet siden bakgrunnen for denne proposisjonen er Europarådets konvensjon av 8. november 2001. Den er ratifisert av de fleste land i Europa, samt USA, Canada og Japan. Norge undertegnet konvensjonen 23. november 2001.

Komiteen ser viktigheten av å bekjempe datakriminalitet siden dette er kriminalitet med et stort skadepotensial samtidig som oppdagelsesrisikoen er lav.

Datainnbrudd - Straffeloven § 145 annet ledd

Komiteen er videre enig i at dagens lovgivning ikke er fullgod på alle områder, ikke minst i forhold til at den som innehar datainformasjon må sørge for beskyttelse mot innsyn fra uberettigede før et misbruk regnes som straffbart. Det vises her til vilkåret om såkalt beskyttelsesbrudd i gjeldende bestemmelse om datainnbrudd i straffeloven § 145 annet ledd. Komiteen vil i den anledning vise til deler av uttalelsen fra Økokrim som blant annet sier at:

"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 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.

Etter vår oppfatning bør straffeloven inneholde en regel om rettsstridig adgang til data som er lagret eller som er under overføring. Beskyttelsesbrudd, skadeforvoldelse eller vinnings hensikt bør være straffskjerpende omstendigheter."

Komiteen foreslår etter dette å fjerne vilkåret om beskyttelsesbrudd i straffeloven § 145 annet ledd, og fremsetter på denne bakgrunn følgende forslag:

"I lov 22. mai 1902 nr. 10 Almindelig borgerlig Straffelov gjøres følgende endring:

§ 145 annet ledd skal lyde:

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

Ulovlig spredning av tilgangsdata - artikkel 6

Komiteen ser det prinsipielle i problematikken rundt det å kriminalisere forberedelseshandlinger og det å være i besittelse av "datavirus, hackerverktøy o.l." Komiteen ser at det også blant høringsinstansene er tydelige forskjeller i hvorvidt dette bør kriminaliseres. Komiteen vil vise til uttalelser fra henholdsvis Oslo politidistrikt og Økokrim. Oslo Politidistrikt begrunner sitt syn om ikke å kriminalisere slike handlinger på følgende måte:

"Oslo politidistrikt viser til Datakrimutvalgets begrunnelse, og er enig i at man bør benytte reservasjonsadgangen i artikkel 6. Kriminalisering av hardware/software som kan tenkes å skulle brukes til straffbare handlinger eller er egnet til dette, er betenkelig. En kriminalisering på dette feltet vil medføre økt kontroll (også fra private aktører med opphavsrettsinteresser) og mistenkeliggjøring av borgerne."

Økokrim sier derimot at slike handlinger bør kriminaliseres fordi

"... gjerningene påfører samfunnet enorme kostnader og underminerer blant annet den tillit som er nødvendig for realisering av den politiske målsetting om utvikling av e-handel… Det antas at klare regler

i seg selv vil kunne ha en preventiv effekt i forhold til tilgjengeliggjøring, siden en del av denne aktiviteten er basert på at gjerningsmennene opplever at de opererer i et straffritt område, i høyden en juridisk gråsone, slik at risikoen for strafforfølgning er minimal."

Komiteens flertall, alle unntatt medlemmene fra Høyre og Kristelig Folkeparti, vil påpeke 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. På denne bakgrunn fremmer flertallet følgende forslag:

"I lov 22. mai 1902 nr. 10 Almindelig borgerlig Straffelov gjøres følgende endring:

Ny § 145b skal lyde:

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.

Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade.

Medvirkning straffes på samme måte."

Flertallet ber imidlertid om at arbeidet tilknyttet problemstillingen rundt forberedelseshandlinger og det å være i besittelse av "datavirus, hackerverktøy o.l" fortsetter.

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.

Disse medlemmer fremmer derfor proposisjonens forslag:

Ny § 145b 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.

Straffeprosessuelle spørsmål

Komiteens flertall, alle unntatt medlemmene fra Høyre og Kristelig Folkeparti, vil i forbindelse med forslaget til ny § 215 a i straffeprosessloven peke på den usikkerhet som kan oppstå i forbindelse med uberettiget bruk av andres nettverk. Det er i dag mange steder svært enkelt å koble seg opp via andres nettverk. Selv om det er enkelt å identifisere hvilken datalinje som er brukt, er det dermed ikke alltid like enkelt å pålitelig identifisere hvem det er som har brukt denne linja.

K o m i t e e n har utover dette ingen merknader til den fremlagte proposisjon ,og slutter seg til de øvrige forslag.

3. FORSLAG FRA MINDRETALL

Forslag fra Høyre og Kristelig Folkeparti:

Ny § 145b 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.

4. KOMITEENS TILRÅDING

K o m i t e e n har for øvrig ingen merknader, viser til proposisjonen og rår Odelstinget til å gjøre slikt

v e d t a k t i l l o v

om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi
(lovtiltak mot datakriminalitet)

I

Lov 22. mai 1902 nr. 10 Almindelig borgerlig Straffelov (straffeloven) endres slik:

I § 12 første ledd nr. 3 bokstav a føyes §§ *145 annet ledd og 145b* til i opplistingen.

§ 145 første ledd skal lyde:

Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder *eller begge deler.*

§ 145 annet ledd skal lyde:

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

Ny § 145b skal lyde:

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.

Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade.

Medvirkning straffes på samme måte.

II

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) endres slik:

Ny § 199a skal lyde:

Ved ransaking av et datasystem kan politiet pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet.

Brudd på opplysningsplikten som begås av andre enn den siktede, straffes etter straffeloven § 339 nr. 1.

Ny § 215a skal lyde:

Påtalemyndigheten kan som ledd i etterforskning gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis.

Pålegg om sikring av data i en sending som besittes av en tilbyder av tilgang til elektroniske kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, kan bare gis dersom vilkårene i første ledd er oppfylt og det er grunn til å tro at det er begått en straffbar handling.

Den som har rådigheten over de data som omfattes av sikringspålegget, skal underrettes om pålegget. En mistenkt skal underrettes straks dataene er sikret og han får status som siktet i saken. For øvrig skal underretning gis straks dataene er sikret.

Sikringspålegget gjelder for et bestemt tidsrom, som ikke må være lenger enn nødvendig og høyst 90 dager om gangen. Dersom sikringspålegget gis etter anmodning fra fremmed stat, gjelder pålegget for minst 60 dager. § 197 tredje ledd, § 208 første og tredje ledd og § 216 i gjelder tilsvarende.

Den pålegget retter seg mot, skal etter begjæring utlevere de trafikkdata som er nødvendige for å spore

hvor dataene som omfattes av sikringspålegget kom fra og hvor de eventuelt ble sendt til.

III

Samtykke til ratifikasjon

Stortinget samtykker til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

IV

Ikraftsetting

Loven trer i kraft straks.

Oslo, i justiskomiteen, den 17. februar 2005

Trond Helleland
leder

Jan Arild Ellingsen
ordfører