Oslo, 24.11.2001

Elektronisk Forpost Norge
c/o Thomas Gramstad
Pb. 2631 Solli
0203 Oslo

Nærings- og handelsdepartementet
Postboks 8014
Dep 0030 Oslo

Elektronisk Forpost Norges høringsuttalelse til "Grunnlagsdokument for Nasjonal strategi for informasjonssikkerhet" (Heretter kalt "Grunnlagsdokumentet" eller bare "GD") :

## Generelle og innledende betraktninger

Informasjonssikkerhet er et omfattende og mangefasettert felt, og knapt noen vil kunne si seg uenig i at arbeidet for å etablere og bevare en adekvat sikkerhet i elektronisk kommunikasjon og i de ulike datasystemer bør være et sentralt prioriteringsområde i den politiske planlegning og utgjøre en bærebjelke i planleggingen av IT-samfunnets infrastruktur.

Både den i Grunnlagsdokumentet sterkt vektlagte verdiskapning som rimeligvis foregår både i privat og offentlig sektor, samt generell informasjonsbehandling og enkeltindividenes private kommunikasjon, foregår i økende utstrekning ved hjelp av informasjonsteknologi. Det er uten videre klart at systemer som har en så stor betydning for vårt samfunn og hele vårt sosiale liv vil være utsatte. Når betydningen og kritikaliteten av en prosess eller et fenomen øker, øker samtidig sårbarheten. Det er i det hele tatt intet brennbart spørsmål at beskyttelse av samfunnets IT-infrastruktur er en udiskutabel nødvendighet i den type samfunn vi har. Elektronisk Forpost Norge slutter derfor opp om Grunnlagsdokumentets erklærte hovedmålsetninger som uttrykt på side 7 og 8 under punkt 1.3 i GD, vi vil uten reservasjon tiltre den omsorg for å bøte på og motvirke sårbarhet som formuleres på side 21 under 3.6, likeledes er vi helt på linje med de situasjonsbedømmelser som uttrykkes i punkt 4.1-4.11, på samme måte som vi forbeholdsløst støtter opp om formålet om å ivareta samfunnssikkerheten som definert på side 31 under 5.1.1. De øvrige situasjonsbeskrivelser og forslag til tilnærmingsmåter og løsninger for å møte de forestående IT-sikkerhetsutfordringer har vi i hovedsak også funnet å kunne slutte oss til.

## "Sikkerhet" et vidt begrep

Ikke desto mindre har vi funnet grunn til å knytte kritiske kommentarer til premissene for enkeltdeler av de metoder som i GD forespeiles tatt i bruk i informasjonssikringsarbeidet.

Nettopp fordi "sikkerhet" er et begrep som omfatter så mange aspekter og berører så mange sektorer, individer og interesser i et informasjonsteknologisk basert kommunikasjonssamfunn, er det av den største betydning å påse at hensynet til visse

grunnleggende verdier og rettigheter i vårt samfunn ikke helles ut med badevannet under henvisning til isolert sett gode og aktverdige formål som, når de søkes gjennomført, lett resulterer i at man innfører tiltak som kan ha til dels meget alvorlige om enn uforutsette skadevirkninger for befolkningen og ikke minst for det i et hvert utviklet samfunn så uvurderlige og helt nødvendige tillitsforholdet mellom borgere og myndigheter. Det er på dette punktet at Elektronisk Forpost Norge (EFN) vil fremføre sterke advarsler mot visse sider av den strategi som er skissert i Grunnlagsdokumentet.

Konkret vil vi rette søkelyset mot deler av de tiltak som foreslås mot hva man på side 15 under 3.1 betegner som "anslag fra kriminelle eller terrorister." Dette vil bli behandlet og utdypet nedenfor, men la oss nå ta utgangspunkt i den helt korrekte konstateringen på side 41 under 5.2.1, hvor det avslutningsvis i en drøfting av "grenseoppganger i det sektorovergripende ansvaret for IT-sikkerhet," hvor det sies at "IT-sikkerhet har flere dimensjoner enn sårbarhet, skadeforebygging og skadebegrensing. Tillits- og utviklingsdimensjonen er like viktig og spesielt viktig i overgangen til verdiskaping i et kunnskapsbasert samfunn."

Tillit er viktig, endog avgjørende viktig, og dette har gyldighet i flere sammenhenger enn de som har direkte forbindelse med hva vi gjerne forstår med "datasikkerhet."

## Hva er "sikkerhet," og hva skal beskyttes?

Grunnlagsdokumentet gir en god beskrivelse av dette, og de analyser og prioriteringer som der fremkommer sammenfaller som nevnt i stor grad med EFNs synspunkter. Imidlertid vil vi rette søkelyset på en svært sentral del av begrepet IT-sikkerhet, som synes å ha fått en i beste fall stemoderlig behandling i det utredningsarbeide som i regi av Nærings- og handelsdepartementet har blitt foretatt med assistanse fra en Justisdepartement-ledet styringsgruppe. Vi sikter her til personvernhensynet.

## Personvernet

I hele GD forekommer ordet "personvern" to ganger, og ikke i noen av tilfellene ble det knyttet an til de etter vår oppfatning aller største utfordringene for personvernet.

På side 61, under "Tilpasning av regelverk" står følgende å lese om "Hjemler for å lette politiets etterforskning av datakriminalitet":

For å lette politiets arbeid med avdekking og straffeforfølging av datakriminalitet må det arbeides videre for å gjennomføre:

* lovpålagt loggføring av bruk av visse Internett-tjenester og krav om identifisering for bruk av slike tjenester, evt. også tilknytning til ISP-er

* hjemmel til å pålegge forlenget lagringstid

* internasjonal utveksling av informasjon om oppkoblinger (trafikkdatatilgang iht. CC-konvensjon

Det er med dyp beklagelse vi i EFN registrerer at de gamle men etter vår mening ikke spesielt gode eller aktverdige målsetningene om generell lovpålagt loggføring av Internett-brukeres trafikkdata og lagring av disse loggene på ny har blitt vekket til live, og det i en så vidt sterk formulering som at man sier at "...må det arbeides videre for å gjennomføre..."

Dette vitner om en sterk intensjon, og er meget foruroligende. Som kjent er kravet om å loggføre trafikkdataene om helt vanlige menneskers aktivitet på Internett langt i fra nytt. Spesielt representanter for Økokrim har fungert som pådrivere for et lovpåbud om slik registrering og lagring av trafikkdata fra vanlige menneskers bruk av Internett, med den hensikt å oppnå sporbarhet av hvilke Internett-sider man besøkte under "surfingen" samt av e-postkommunikasjon. Vi er avhengig av at samfunnets datatjenester fungerer og er pålitelige, og at de beskyttes mot datainnbrudd og andre kriminelle anslag. Det er imidlertid etter EFNs syn en stor og svært farlig misforståelse å tro at ivaretakelsen av datasikkerhet har som forutsetning at vi aksepterer kontroll av hva enkeltindividet foretar seg på Internett, og dermed overkjører personvernhensynene.

En fundamental og ufravikelig forutsetning for personvern er retten og muligheten til selvvalgt anonymitet og ikke-sporbarhet i vanlige borgeres elektroniske kommunikasjon. Urovekkende er det når det gjentatte ganger kommuniseres påstander om at dersom ikke alle enkeltindividers elektroniske kommunikasjon overvåkes og gjøres sporbar, blir Internett til et "fristed for kriminelle," som det retorisk har blitt hevdet av enkelte som er av den mening at kriminalitetstruselen på Internett ikke kan møtes effektivt uten generell elektronisk overvåkning.

En slik kontroll av befolkningen ville innebære en de facto kriminalisering av samtlige borgere, fordi den har som uuttalt underliggende premiss at "vi må kontrollere og spore deg i tilfelle du gjør noe galt." Tilfanget av informasjon om hver enkelt borgers bevegelser på nettet ville over tid bli meget omfattende, og man ville i et slikt scenario skape en sterk utrygghet og motvilje i befolkningen, med en gradvis underminering av respekten for lov og rett og i verste fall for rettsstaten som sådan. Det bør anses som utvilsomt at en slik omfattende og lovpålagt kontroll fra myndighetenes side over innbyggernes bevegelser på og bruk av Internett representerer en grov integritetskrenkelse av lovlydige borgere.

Opp mot dette synspunktet vil de som ønsker slik loggføring og sporbarhet sette "politiets behov" for å kunne etterforske kriminalitet, og her vil det eksempelvis kunne henvises til de tall som er presentert i GD, og hvor det i følge undersøkelsen "Datakriminalitet i 2001 - en mørketallsundersøkelse" foretatt i fellesskap av Økokrim og Næringslivets sikkerhetsorganisasjon fremgår at i år 2001 ble 62% av alle bedrifter utsatt for datakriminalitet, og det nevnes tall som 7500 gjennomførte datainnbrudd, 500 000 forsøk og ni millioner virusangrep. Ingen vil benekte at dette er betydelige tall, og selv om en leser her bør ta visse forbehold i forhold til at hverken alvorligheten, graden og omfanget av destruksjon eller selve definisjonen på hva de ulike dataangrepene innebærer er nærmere konkretisert, kan det vanskelig nektes for at både næringslivet, offentlige virksomheter og privatpersoner står overfor høyst reelle utfordringer med hensyn til å motarbeide datakriminalitet.

Dermed er det likevel ikke gitt at løsningen betinger at man ved lov fratar mennesker retten til å ferdes anonymt på nettet eller å kommunisere via e-post uten at politiet skal kunne følge med på aktiviteten. Nettopp når vi som samfunn står overfor slike

utfordringer som tilfellet beviselig er når det gjelder datakriminalitet, er det av særdeles stor viktighet at man mobiliserer vilje og evne til å unngå å handle overilet og gjennomføre drastiske tiltak som medfører store og unødige belastninger og skadevirkninger for det samfunn man i utgangspunktet ønsker å verne om. I et vidt perspektiv er tillitsforholdet mellom eksempelvis politiet og befolkningen helt vesentlig for å kunne motvirke kriminalitet. Da vil det virke meget mot sin hensikt dersom detaljene om den vanlige borgers elektroniske kommunikasjon skal gjøres sporbar. Kravet om at logger fra borgernes Internett-aktivitet skal være tilgjengelig for myndighetene i lengre tid er et eksempel på et slikt tiltak som kan sies å være om ikke nødvendigvis uoverveid, så ubetinget utilstrekkelig analysert i sine konsekvenser enn si veid opp mot de hensyn til og den respekt for privatliv, personvern og anonymitet som innbyggerne i en genuin rettsstat bør nyte godt av. Dersom myndighetene forlanger å kartlegge og få muligheten til detaljert informasjon om den jevne borgers kommunikasjonshandlinger, dreier dette seg i realiteten om noe så alvorlig som et brudd på den stilltiende men like fullt alment aksepterte sosiale kontrakt som i et fritt og demokratisk samfunn eksisterer mellom myndigheter og borgere. Det blir i desto høyere grad et alvorlig tillitsbrudd ettersom elektronisk kommunikasjon har og vil få stadig mer omfattende betydning og plass i samfunnet og i det enkelte individets hverdag. Dette forholdet understreker det graverende i at det reises krav om at ordinære borgere skal underkastes lovpåbudt overvåkning på Internett, herunder overvåkning av elektronisk post.

Her kan det være på sin plass å peke på at ethvert krav om å kontrollere borgernes adferd på en så gjennomgripende måte som logging og oppbevaring av trafikkdata fra alles bevegelser på Internett vil innebære, står i skarp motstrid til hva de aller fleste lovlydige borgere vil mene er den i et demokrati selvfølgelige rett til å bevege seg fritt uten å bli kontrollert av myndighetene. Slik vil det også bli oppfattet av mange, sannsynligvis de fleste, mennesker. En må derfor regne med at pådrivere bak bestrebelser på å få innført en slik overvåkning vil benytte seg av en velbrukt politisk taktikk: Å lansere forslag som de på forhånd regner med ikke vil bli vedtatt, hvorpå de lanserer et annet og tilsynelatende mindre drastisk forslag med den tanke om at dette vil gå gjennom fordi det sett i lys av det foregående og mer radikale forslag fortoner seg som "moderat" og derfor har mulighet til å bli akseptert.

Vi vil nevne dette momentet fordi EFN ønsker å understreke at det i denne sak dreier seg om et "tertium non datur"-tilfelle, hvor det i virkeligheten kun foreligger to muligheter: Enten gis Internett-leverandører og teleselskaper lovlig mulighet til å oppbevare trafikkdata i så lang tid som det er nødvendig for å ivareta fakturerings- og betalingsrutiner, eller de samme virksomhetene pålegges å lagre trafikkdata over lengre tid slik at myndigheter og politi skal kunne kartlegge hver enkelt brukers bevegelser inn i fremtiden. En kan anta at det her vil bli forsøkt med å lansere tilsynelatende kompromissforslag mht. varigheten av den lovpålagte lagringen man ønsker, og det er derfor viktig at de som ikke ønsker å gi myndighetene denne kontrollmakt er oppmerksomme på denne form for taktikk og fastholder at det må være en ufravikelig rett i et demokratisk og forutsetningsvis fritt samfunn å som lovlydig borger være fritatt for myndighetenes overvåkning og kontroll av ens bevegelser, og da spesielt på en så sentral arena som Internett har blitt og vil komme til å være. Vårt standpunkt er at ingenting annet er akseptabelt enn at elektroniske trafikkdata slettes etter at inneværende faktureringsperiode er betalt for av kunden.

Man bør imidlertid være forberedt på at innvendinger mot de ovenstående resonnementer vil bli reist, og at det fra overvåkningsinteressenes side vil bli hevdet at

den beskrevne kontroll og sporbarhet er en forutsetning for at de i Grunnlagsdokumentet oppsatte målsetninger for informasjonssikkerhet skal kunne realiseres.

Til dette er å si at for det første virker det lite rimelig å snakke om "informasjonssikkerhet" uten å ta med i betraktningen den enkelte borgers frihet og rett til å slippe å bli påtvunget en slik kontroll som blant annet Økokrim dessverre har gjort seg til talerør for. Reelt personvern for en ikke-kriminell borger forutsetter mulighet til anonymitet og frihet fra overvåkning. Det bør ikke kunne aksepteres at de som ønsker å øke myndighetenes kontrollmakt over befolkningen utdefinerer frihet fra overvåkning som en del av personvernbegrepet. Grunnlagsdokumentets store svakhet er at man ikke problematiserer den realitet at dersom myndigheter skal ha utvidede fullmakter og flere muligheter til innsyn i vanlige menneskers liv og levnet, innskrenkes de sistnevntes frihet og rettigheter tilsvarende. I denne forbindelse kan det ikke betraktes som relevant at vi lever i et land med et demokratisk valgt parlament. En omfattende kontroll overfor vanlige mennesker er i seg selv et maktovergrep, og visse kretsers krav om å følge med på hva vi gjør elektronisk, og dertil spore våre bevegelser i lang ettertid, bør betraktes som hva det er, nemlig et intolerabelt anslag mot publikums privatliv.

For det annet, og sett fra det overordnede samfunnssikkerhetssynspunkt om mulig enda viktigere: Premisset om at det er påkrevet å iverksette en slik storstilt overvåkning av innbyggerne er høyst sannsynlig uholdbart. En seriøs satsing på effektive tilgangskontroll- og autentiseringssystemer, samt bedring av sikkerheten lokalt i den enkelte virksomet og den enkelte husholdning er her den riktige medisin. Grunnlagsdokumentet tar da også til orde for det samme, og understreker med all rett viktigheten av slike teknikker, rutiner og prosedyrer for ivaretakelse av sikkerhet. Vi finner at det i det hele tatt ikke er sannsynliggjort at overvåkning av befolkningen er et nødvendig tiltak for å bedre IT-sikkerhet. Tvert i mot, med omfattende elektronisk kontroll fratas den enkelte borger sin rett og mulighet til å holde sin kommunikasjon skjermet fra myndighetenes innsyn, og derigjennom undermineres også individenes datasikkerhet i videste forstand.

I tillegg kommer også problematikken med at når det forekommer langtidslagring av logger, vil ikke bare politiet og myndighetene, men også kriminelle, kunne få tilgang til disse loggene og bruke dem til angrep mot bedrifter, samfunnet eller enkeltpersoner. Dette alene er en vektig grunn til å avvise lagring av trafikkdata, men her er det altfor lett å bevege seg inn på et sidespor hvor man diskuterer sannsynlighet og hvor overvåkningsinteressene avgir forsikringer om at "vi skal klare å lagre trygt." Derfor ønsker vi likevel å nedtone dette momentet noe i forhold til det prinsipielle: at myndighetene generelt ikke må gis adgang til å innhente informasjon om hva lovlydige borgere foretar seg, og ganske spesielt ikke ha tilgang til lagrede logger over aktiviteten.

## Mer om datakriminalitet og brukbare strategier

Enkelte vil påstå at fravær av både sanntidsovervåkning og sporbarhet i ettertid kommer til å gjøre Internett til et fristed for kriminelle. Slike utspill bør avvises. Spørsmålet er ikke om man skal etterforske kriminelle personer og organisasjoner som påviselig har gjort seg skyldig i lovbrudd og farlig virksomhet. Dette kan ingen ha noe i

mot. Spørsmålet er om vi skal godta at alles elektroniske kommunikasjon skal kunne registreres og lagres slik at myndighetene og deres maktapparat skal kunne spore alle detaljer om vår e-post, vår nettsurfing og våre telefonsamtaler i lang tid fremover. Denne problematikken har naturligvis også en internasjonal dimensjon, da det er en mulighet for at EU-organer kan komme til å påby slik overvåkning innen EU/EØS-området, slik at Grunnlagsdokumentets ytring på side 52 under 6.1.6 om at "Regler fra EU, OECD, NATO og FN må tas hensyn til" kan få en mindre positiv betydning. I så fall blir det en høyt prioritert politisk oppgave for borgerrettighetsorganisasjoner å arbeide for å etablere politisk motstand mot overvåkning slik at det internasjonale lovverk over tid kan endres slik at det reflekterer borgernes interesser. Både på det overnasjonale plan og innenfor hvert enkelt land må det arbeides for å avgrense myndighetenes kontrollmakt.

Når det gjelder påstandene om at kriminalitetsbekjempelse nødvendiggjør streng kontroll med enkeltmenneskers aktivitet på nettet, er å si at kriminell aktivitet typisk er mulig å påvise definert der den utøves, og materiale som barneporno eller annet lovstridig materiale på nettet betinger heller ikke noen generell overvåkning.

Vi nevner disse tingene som relevante momenter fordi de ofte trekkes frem i diskusjonen. Den som legger ut ulovlig materiale, må nødvendigvis gjøre det tilgjengelig, og dermed kan det påvises hvis politiet er sitt ansvar bevisst og søker/surfer manuelt eller med dertil egnede automatiserte programmer etter det materiale man mener å ha grunn til å mistenke at befinner seg på nettet. Internasjonalt har slike søk blant annet ført til at tusentalls sider av opphavsrettsbeskyttet materiale har blitt avslørt og stengt, noe som gir ytterligere vekt til konklusjonen om at en overvåkning av den enkeltes surfeaktivitet eller e-postkommunikasjon ikke er nødvendig for kriminalitetsforebyggelse.

Hva angår terrorismerisikoen som også er hyppig brukt som argument og derfor også bør nevnes, er EFNs posisjon at det på ingen måte fremstår som sannsynlig at elektronisk overvåkning av den jevne borger vil "treffe" terrorister med så stor sikkerhet at dette er noen holdbar rettferdiggjørelse. Vår bedømmelse er at den hypotetiske etterretningsmessige gevinst må veies mot de meget alvorlige ulemper som samfunn og individ påføres ved at man i terroristfrykt skaper et kontrollsamfunn, og at denne avveiningen tilsier at generell elektronisk sporbarhet med loggføring av elektronisk aktivitet må avvises som ledd i en sikkerhetsstrategi. Som svar til mulige innvendinger om at logging og sporbarhet er påkrevet fordi eksempelvis ikke alle datainnbrudd avsløres umiddelbart, må understrekes den store viktigheten av at effektive stedlige IT-sikkerhetstiltak utvikles og iverksettes.

EFN finner grunn til å konkludere med at det er lite eller ingenting som tilsier at en overvåkning av alle borgerne med lagring av diverse trafikkdata er noen forutsetning for å bekjempe hverken ordinær kriminalitet, datakriminalitet eller terrorisme. Derimot er ønsket om å iverksette slike tiltak et uttrykk for en fundamental kontrollvilje, hvor man ganske tydelig signaliserer at "Vi stoler ikke på dere, så vi ønsker å loggføre alt dere gjør." Her bør alle parter være bevisste om at innenfor rammen av en honnørverdi som "demokrati" gis det vidt spillerom for ulike former for mer eller mindre subtil undertrykkelse og innskrenkning av rettigheter og bevegelsesfrihet for borgerne i et i navnet demokratisk samfunn. Menneskerettigheter og ytringsfrihet er elementære og alment aksepterte og gitte rammebetingelser, men garanterer ikke i seg selv at det være seg maktbalansen er sunn eller at individenes rettigheter vis-a-vis myndighetene er ivaretatt på optimalt vis. Utvidede fullmakter til

å kontrollere borgerne forrykker maktbalansen i faretruende grad, og vi vil derfor på det aller sterkeste måtte advare mot en slik linje.

Vi er på det rene med at det vil bli hevdet at "i et demokratisk samfunn foreligger ingen risiko." Til dette vil vi svare at demokratiet som nevnt aldri er gitt en gang for alle. Dertil bør det i et demokratisk samfunn være en selvfølgelighet at borgernes fysiske så vel som elektroniske bevegelser ikke skal være mulig å detaljovervåke og/eller spore for myndighetene. Hverken terrorisme eller andre uønskede fenomener rettferdiggjør at befolkningen som helhet skal påtvinges ridig kontroll og universell sporbarhet.

## Autentisering og bruk av elektroniske signaturer

På side 65 i GD, under punkt 8, fremføres "Forslag vedrørende en samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring av sensitiv informasjon."

Man nevner PKI (Public Key Infrastructure)-teknologi som en realistisk strategi for å realisere det ovennevnte. EFN vil støtte denne krypteringsteknologien, og er derfor enig i de målsetninger for Nasjonalt PKI-forum som er beskrevet. Vi vil kun ta et forbehold: Det må være et ufravikelig krav at denne type systemer bygges opp slik at de ikke forutsetter bruk av bestemte programvare- eller maskinvareplattformer, men kan benyttes av brukere med alle kjente forekommende operativsystemer og datamaskiner.

Utover hva som her er nevnt, har vi ingen flere ting å anføre.

Vennlig hilsen

Elektronisk Forpost Norge
v/ Per Inge Østmoen

Per Inge Østmoen