9 Hur bör en reglering utformas närmare?

9.1 Utgångspunkter för en lagreglering

Vårt förslag: En särskild ny lag som reglerar administrationen av en nationell toppdomän för Sverige bör skapas. Lagens syfte skall vara att säkerställa att administrationen av en nationell toppdomän utförs på ett robust, säkert och effektivt sätt i allmänhetens intresse.

En ny lagreglering bör utformas med GAC:s principer som underlag. Dessa ger, som beskrivits i kapitel 5, endast det övergripande ramverket för hur administrationen av en nationell toppdomän skall vara uppbyggd. Principerna reglerar t.ex. varken de närmare förutsättningarna för namntilldelning och registrering av huvuddomännamn under toppdomänen eller tvistlösnings- och tillsynsverksamheternas närmare utformning.

En reglering av nu nämnda frågor bör ske genom lag. Av lagen bör framgå de yttre kriterierna för administrationen av den nationella toppdomänen för Sverige. Lagregleringen bör så långt möjligt anpassas till svensk lagstiftningstradition såvitt gäller innehåll och struktur. Det är mot denna bakgrund varken möjligt eller ens önskvärt att fullständigt överföra GAC:s principer till nationell lagstiftning.

9.1.1 Skall en ny lag skapas?

Tidigare har vi konstaterat att administrationen av den nationella toppdomänen för Sverige bör regleras i en offentligrättslig reglering. En fråga att ta ställning till är om den nya lagregleringen skall ske genom en ny lag för domännamnshantering eller i redan befintlig eller beslutad lagstiftning, t.ex. lagen om elektronisk kommunikation (EkomL).

Administrationen av en nationell toppdomän är i allt väsentligt av infrastrukturell karaktär och avser inte innehåll i elektronisk kommunikation. Infrastruktur för elektronisk kommunikation regleras huvudsakligen i den nyligen beslutade EkomL som kommer att träda i kraft den 25 juli 2003. Det kan därför vid en första anblick tyckas lämpligt att den nya regleringen av administrationen av toppdomänen *se* samordnas och införs i EkomL.

Mot en samordning talar emellertid att administrationen av toppdomänen *se* utgör en infrastrukturell reglering av speciell karaktär, som i allt väsentligt saknar beröringspunkter med de övriga infrastrukturella frågor som EkomL avser. Att införa regler om administrationen av en nationell toppdomän i EkomL kan därför leda till att det uppkommer besvärliga frågor om tillämplighet av olika bestämmelser i EkomL på sådan verksamhet. Med hänsyn till detta och då det inte kan anföras några bärande skäl mot att särreglera administrationen av en nationell toppdomän finner utredningen att regleringen bör införas i en särskild lag.

9.1.2 Lagens syfte

Enligt våra direktiv skall vi undersöka möjligheterna att genomföra GAC:s principer, särskilt artikel 5 som rör statens roll, genom en offentligrättslig reglering och lämna de författningsförslag som anses nödvändiga för att möjliggöra statlig tillsyn av principernas efterlevnad.

I artikeln slås fast att Internets namnsystem är en offentlig nyttighet i den meningen att dess funktioner måste administreras i allmännyttans intresse samt att staten är den högsta företrädaren för detta intresse i det land eller det område för vilket en nationell toppdomän har delegerats. Det är alltså statens uppgift att tillse att toppdomänen administreras på ett allmännyttigt sätt.

I tidigare kapitel konstaterade utredningen också att en väl fungerande Internetanvändning utgör ett viktigt samhälleligt intresse som kräver att staten kan garantera åtkomligheten av samhällsnödvändiga resurser under en nationell toppdomän för Sverige.

För att säkerställa dels att verksamheten bedrivs i allmänhetens intresse, dels åtkomligheten av de nämnda samhällsnödvändiga resurserna bör lagen ange vissa kriterier som skall vara uppfyllda i verksamheten att administrera en nationell toppdomän för Sverige.

Dessutom måste en kontrollmöjlighet skapas för att tillse att kriterierna verkligen uppfylls.

De grundläggande syften som lagen skall säkerställa bör komma till uttryck i en särskild ändamålsbestämmelse. Det bör där klargöras att verksamheten skall bedrivas i allmänhetens intresse. Den lokala anknytningen erhålls genom att lagen endast gäller verksamhet som bedrivs i Sverige. I ändamålet ligger även att administrationen skall ske på ett robust, säkert och effektivt sätt. Vad som närmare avses i dessa hänseende och på vilket sätt detta skall ske återkommer vi till nedan under bl.a. avsnitt 9.2.1 och 9.2.2 som behandlar teknisk drift och driftssäkerhet.

Huvudsyftet med den lag vi föreslår är alltså att säkerställa att administrationen av den nationella toppdomänen *se* utförs på ett sätt som ger ett robust och effektivt Internet där säkerhet och jämlik tillgång till domännamn skall vara ledstjärnor. Genom att skapa möjlighet för staten att kontrollera och vid behov ingripa för att tillse att de uppställda kriterierna uppfylls, främjas det högre och övergripande syftet att öka och förbättra informationssamhällets serviceutbud över Internet.

9.2 Närmare om regler för den administrativt ansvarige för en nationell toppdomän för Sverige

Vårt förslag: Den föreslagna lagen skall inte reglera hur den administrativt ansvarige för en nationell toppdomän för Sverige skall utses. Lagen bör dock innehålla ett krav på att den administrativt ansvarige skall ha sitt hemvist eller säte i Sverige.

I lagen skall fastslås den administrativt ansvariges skyldigheter vid verksamhetens bedrivande. Verksamheten skall bedrivas bl.a. med beaktande av allmänhetens intresse av effektiv Internetanvändning samt internationella överenskommelser som Sverige anslutit sig till och bestämmelser som antagits med stöd av Fördraget om upprättandet av Europeiska gemenskapen.

Vidare skall den administrativt ansvarige tillhandahålla tillsynsmyndigheten en säkerhetskopia av för verksamheten relevanta registerdata och, vid uppdragets upphörande, föra över sådana data till ny administratör.

9.2.1 Några definitioner

För att klargöra de begrepp som används och ligger till grund för bestämmelserna i GAC:s principer anges i artikel 3 i principerna vissa definitioner. Av dessa är det särskilt begreppen nationell toppdomän och uppdragstagare, som är av intresse.

Med en *nationell toppdomän* förstås en domän på den högsta nivån i det internationella domännamnssystemet (DNS) som har tilldelats i enlighet med tvåbokstavskoderna i dokument SS EN ISO 3166 1: Landsbeteckningar. För Sveriges vidkommande är den officiella beteckningen enligt standarden "se". Den nationella toppdomän som träffas av denna definition är alltså toppdomänen *se*. Denna definition bör överföras till en ny lag dock utan att binda upp definitionen till beteckningen enligt nämnda ISO-standard. Även andra i framtiden tänkbara beteckningar för Sverige bör alltså kunna omfattas av definitionen.

Med *uppdragstagare* eller "delegee" avses enligt GAC:s principer en organisation, ett bolag eller en fysisk person som förordnats av respektive stat att utöva det offentliga förtroendeuppdraget att hantera en nationell toppdomän och därefter har erkänts för det ändamålet genom ett avtal mellan ICANN och uppdragstagaren. Definitionen har utsatts för en del kritik bl.a. för att den inte omfattar de som före det att principerna togs fram fått och fortsatt utför förtroendeuppdraget utan ett formellt förordnande. Det har därför framförts att begreppet bör bytas ut mot registreringsenhet, "ccTLD Registry", och att definitionen vidgas till att avse den som är ansvarig för hanteringen och administrationen av en nationell toppdomän samt att det anges att den ansvarige kan vara formellt förordnad eller erkänd av den relevanta staten.

I Europaparlamentets och rådet förordning (EG) nr 733/2002 av den 22 april 2002 om inrättande av toppdomänen .eu används begreppet "registreringsenhet". Det definieras som den enhet som fått i uppdrag att organisera, administrera och förvalta toppdomänen *eu*, vilket omfattar driften av tillhörande databaser och offentliga söktjänster, registrering av domännamn, drift av registreringsenheten för domännamn, drift av toppdomänens registreringsenhets namnservrar samt fördelning av zonfiler för toppdomänen.

Även om skäl talar för att i möjligaste utsträckning vidmakthålla en enhetlig begreppsbildning, speciellt i Europa, finns det anledning att i viss mån ta fasta på de synpunkter som lämnats på definitionen av uppdragstagare i GAC:s principer. Vi anser i likhet med

dessa att begreppet ”uppdragstagare” inte i tillräcklig utsträckning anger det ansvar som verkligen åvilar den som utför det nämnda förtroendeuppdraget och därför inte bör användas i en ny lag. Det är vidare enligt utredningens mening mer naturligt att i lagtexten använda begreppet ”administratören” om den som är administrativt ansvarig än begreppet ”registerenhet”. Sistnämnda begrepp är i någon mån missvisande eftersom det inte endast är fråga om att registrera namn. I uppgiften att administrera en nationell toppdomän ingår även att säkerställa att denna fungerar tekniskt m.m.

9.2.2 Hur skall den administrativt ansvarige för den nationella toppdomänen för Sverige utses?

Av vad som tidigare framgått är det grundläggande skälet för en offentligrättslig reglering att tillse att administrationen av den nationella toppdomänen sköts på ett säkert, robust och effektivt sätt. Det är alltså själva verksamheten som sådan som skall regleras. En fråga för utredningen att ta ställning till är om det finns skäl att ändå närmare reglera hur den som skall administrera toppdomänen skall utses.

Fördelen med att i lag ange hur en administrativt ansvarig skall utses är, med hänsyn till att uppgiften gäller att administrera en för samhället och allmänheten viktig funktion, att det skapas en legitimitet och öppenhet i tillsättningsförfarandet. Dessa fördelar vinner ytterligare på att det också kan skapas närmare föreskrifter som klart anger vad som skall uppfyllas för att någon skall kunna komma i fråga för uppgiften. Tillsättningsförfarandet blir på så sätt föremål för en bra genomlyssning. Genom att staten tillsätter eller utser en administrativt ansvarig uppkommer även verkningsfulla möjligheter till sanktioner mot den som inte uppfyller de kriterier som gäller för verksamheten. Den yttersta sanktionen skulle då vara att staten utser någon annan.

Emellertid finns det starka både principiella och praktiska skäl mot att ge staten uppgiften att utse den som skall handha administrationen av en nationell toppdomän. Allmänt kan sägas att de som är ansvariga för administrationen av nationella toppdomäner har som regel erhållit sina uppdrag på olika sätt. Så kan ha skett genom t.ex. formlösa överenskommelser eller genom skriftliga avtal. Som en generell princip gäller dock för administrationen av toppdomänen – såväl nationella som generiska – att den har sin

utgångspunkt i strikt privaträttsliga förhållanden. Sålunda grundas delegationen av den nationella toppdomänen *se* till II-stiftelsen i en privaträttslig överenskommelse mellan ICANN och stiftelsen. Att nationella toppdomäner utvecklats till att administrationen av dem blivit ett allmänt intresse innebär inte i sig att administrationens privaträttsliga karaktär förändrats. Den ökade samhällsbetydelsen av Internetanvändningen har inte visat på behov av förändringar i detta hänseende. Tvärtom talar den utveckling som varit för att frågan om vem som skall administrera den nationella toppdomänen alltjämt bör vara en privaträttslig fråga.

Också från praktisk synpunkt finns det skäl som talar mot att staten skall utse den administrativt ansvarige för administrationen av toppdomänen. De modeller för hur en administrativt ansvarig kan erhålla uppgiften att administrera en nationell toppdomän kräver enligt GAC:s principer dels godkännande av den aktuella staten, dels godkännande och verkställande med hjälp av ICANN och DoC i form av en delegering införd i DNS-roten. Det går alltså inte att genom nationell lagstiftning, som överlåter åt staten att utse vem som skall administrera en nationell toppdomän, säkerställa att ett sådant beslut verkligen kan effektueras, även om det finns en övervägande sannolikhet för att så skall bli fallet.

Avsaknad av lagstiftning innebär inte att staten blir utan inflytande på frågan om vem som skall administrera en nationell toppdomän för Sverige. Det kommer att finnas goda möjligheter att genom avtal och underhandskontakter med ICANN utöva påverkan.

Sammantaget förordar därför utredningen en reglering som inte anger hur den administrativt ansvarige skall utses. Regleringen skall endast avse den verksamhet som en sådan skall bedriva.

9.2.3 Krav på den administrativt ansvarige

Enligt de grundläggande tankarna bakom DNS utgör uppgiften att administrera en nationell toppdomän ett uppdrag i allmänhetens, huvudsakligen den lokala gemenskapens, intresse och innebär en skyldighet att betjäna de som har hemvist i området. I GAC:s principer förordas därför som utgångspunkt en ordning där den administrativt ansvarige har hemvist eller säte i det aktuella området.

Förutom att det av praktiska skäl kan föreligga stora fördelar med att den administrativt ansvarige bedriver sin verksamhet i det område som denne är satt att betjäna finns det även klara juridiska fördelar med en sådan lösning. De regelverk som tillämpas inom Sverige gäller som utgångspunkt endast inom det egna territoriet och svenska resurser. Även om jurisdiktionen kan utsträckas till att omfatta även verksamhet som bedrivs av någon utomlands är det förenat med praktiska svårigheter att genomföra t.ex. tillsyn över verksamheten, om denna inte bedrivs inom det egna territoriet.

En inte oväsentlig omständighet i sammanhanget är vidare att toppdomänen *se*, som ovan konstaterats, har utvecklats till att vara en kritisk resurs för Internetanvändningen i Sverige. Detta förhållande talar med styrka för att den administrativt ansvarige för administrationen av den nationella toppdomänen för Sverige bör ha hemvist i Sverige. Sammantaget finner utredningen alltså att det är välmotiverat att kräva att den administrativt ansvarige har hemvist eller säte i Sverige. Vi förordar därför en sådan reglering i den nya lagen.

Av samma skäl och även med hänsyn till att fråga är om en samhällsviktig funktion som måste förvaltas väl i allmänhetens intresse bör den administrativt ansvarige inte utan anmälan till tillsynsmyndigheten helt eller delvis få uppdra åt annan att utföra uppdraget att administrera toppdomänen. Genom att införa en anmälningsskyldighet möjliggörs för tillsynsmyndigheten att snabbt få en överblick och utöva tillsyn över den till vilken uppdraget har lämnats. Skyldigheten är inte lika långtgående som artiklarna 4.1 och 9.2 i GAC:s principer, som ställer upp ett krav på att staten och ICANN även i dessa fall skall godkänna den som utkontraktering eller utlicensiering skall ske till. Vad ovan anförts om att staten inte bör utse den som skall administrera den nationella toppdomänen, gör sig emellertid gällande även i denna del.

9.2.4 Något om vilka skyldigheter som åvilar den administrativt ansvarige

Av GAC:s principer framgår, som tidigare nämnts, att den administrativt ansvarige är förtroendeman för den delegerade domänen och är skyldig att betjäna personer med hemvist i landet eller området i fråga. Som ett led i detta har denne att hantera den

nationella toppdomänen i den lokala allmännyttans och det globala Internetsamfundets intresse.

Den administrativt ansvarige är även skyldig att administrera den nationella toppdomänen i överensstämmelse med nationell offentlig policy, nationella lagar och bestämmelser samt internationell rätt och tillämpliga internationella avtal. Härmed avses bl.a. reglering med sikte på konkurrens, icke-diskriminering, integritetsskydd samt konsumentskydd. Det kan ifrågasättas vilka moment i artikeln som behöver regleras i en ny lag om administrationen av en nationell toppdomän för Sverige bl.a. mot bakgrund av den befintliga nationella lagstiftning som finns på de angivna områdena. Att en administrativt ansvarig för administrationen av den nationella toppdomänen för Sverige med hemvist eller säte i riket har att tillämpa nationella regler är klart. Det bör dock klargöras i lagtext att skyldigheten även gäller internationella överenskommelser som Sverige har anslutit sig till och bestämmelser som antagits med stöd av Fördraget om upprättandet av Europeiska gemenskapen.

Utöver det anförda är, som nedan kommer att behandlas, den administrativt ansvarige skyldig att medverka till en smidig övergång av administrationen av den nationella toppdomänen vid uppdragets upphörande samt säkerställa att den tekniska driften av toppdomänen sker med erforderliga säkerhetsåtgärder m.m.

Vid tvist bör den administrativt ansvarige tillhandahålla ett effektivt tvistlösningsförfarande. Också till detta återkommer vi längre fram.

9.2.5 Förfarandet vid uppdragets upphörande

I GAC:s principer föreskrivs på ett antal ställen att förfarandet vid uppdragets upphörande bör regleras. Vidare framgår att det skall finnas bestämmelser som vid ett sådant förlopp säkerställer att alla relevanta DNS-data överförs till en förordnad ersättare.

Vikten av att reglera förfarandet vid uppdragets upphörande är speciellt tydlig med hänsyn till de återverkningar en icke fungerande eller verksam administration av den nationella toppdomänen skulle få för Internetanvändningen. Det spelar ingen egentlig roll vilket skälet för uppdragets upphörande är. Det kan visserligen komma att gälla misskötsel av verksamheten men även det förhållandet att en administrativt ansvarig går i konkurs bör omfattas av regleringen.

Eftersom ett upphörande av administrationen av olika skäl kan ske mer eller mindre abrupt, måste det finnas möjlighet att överta administrationen med mycket kort varsel. Vad som i ett första led måste säkerställas är att verksamheten så snart som möjligt kan återupptas av en ersättare. För att så skall kunna ske krävs att ersättaren har tillgång till relevanta DNS-data. Utredningar som PTS bedrivit inom sitt uppdrag att undersöka Internets beroende av funktioner utomlands, t.ex. rapporten Är Internet i Sverige robust, visar att DNS-tjänsten visserligen är uppbyggd på ett sådant sätt med lagring av information att en kortare tids stopp i verksamheten inte behöver påverka Internetanvändningen. När denna information har uppnått sin bäst före datum, Time to Live (TTL), kommer systemet att sakta släckas ner.

Ett sätt att säkerställa den fortsatta driften initialt är att möjliggöra för tillsynsmyndigheten att ha hand om en kopia av relevanta DNS-data.

När en verksamhet upphör bör relevanta DNS-data överflyttas till en ny administrativt ansvarig.

9.3 Särskilt om hur driften av en nationell toppdomän bör regleras

9.3.1 Teknisk drift

Av vikt för en globalt fungerande och effektiv Internetanvändning är att så många användare som möjligt kan nå varandra. För att så skall kunna ske krävs att de system och den utrustning som används inom olika delar av Internet, oavsett var de är belägna, är kompatibla med varandra. Utveckling av tekniska standarder och efterlevnaden av dessa är därför av betydelse.

Med teknisk drift avser vi i detta hänseende genomförandet av den tekniska funktionaliteten i verksamheten. Den tar närmast uteslutande sikte på den s.k. DNS-tjänsten.

9.3.1.1 Vilka tekniska krav på driften ställs upp i dag?

Det är enligt artikel 6.1 i GAC:s principer en av ICANN:s huvuduppgifter att upprätta de tekniska normer och den praxis som skall gälla för hanteringen av det globala DNS. ICANN administrerar i detta syfte ett antal tekniska funktioner för Internet. Dessa funk-

tioner avser bl.a. samordning av tilldelningen av sådana andra tekniska Internetparametrar som är nödvändiga för att bibehålla universell anslutningsbarhet i Internet samt annan verksamhet som är nödvändig för att koordinera vissa funktioner för administrationen av DNS. ICANN skall även utöva tillsyn över tillämpningen av de upprättade tekniska normerna m.m.

Som ett led i uppgiften att tillskapa ett tekniskt kompatibelt, tillgängligt och effektivt Internet skall ICANN bl.a. ombesörja att de auktoritativa master- och slavservrarna för en nationell toppdomän hanteras och vidmakthålls på ett stabilt och säkert vis så att användare inom hela Internetsystemet och alla underdomäner över vilka de utövar administrativ styrning kan slå upp namn inom toppdomänen. Vidare skall ICANN utfärda riktlinjer i fråga om bl.a. samverkansförmåga mellan en nationell toppdomän och andra delar av DNS och Internet samt om toppdomänoperatörens driftsmässiga förmåga och prestanda.

I ICANN:s regi har det tagits fram riktlinjer för den som är administrativt ansvarig för en nationell toppdomän, s.k. Best Practice Guidelines for ccTLD Managers.[1] Av dessa följer – utöver att den administrativt ansvarige är ansvarig för driften av den nationella toppdomänen, inkluderande drift av domännamnsservrarna, och zonfilöverföring – att denne skall uppfylla vissa tekniska krav för verksamheten.

Det första kravet behandlar driftsäkerhetsfrågan och innebär en skyldighet för den administrativt ansvarige att säkerställa att alla DNS-data är tillräckligt skyddade mot skada eller förlust enligt bästa rimliga teknik. Vi återkommer till denna fråga nedan (se avsnitt 9.3.2).

I riktlinjerna ställs även upp krav på att den nationella toppdomänens DNS-tjänst skall vara kontinuerligt tillgänglig. Som en minimireglering, med stöd i RFC 1591 och ICP-1, anges att den administrativt ansvarige för toppdomänen skall dygnet runt tillhandahålla anslutningsmöjlighet avseende Internet Protocol (IP) till namnservrar som ger möjlighet för användarna att nå varandra eller en domännamnsinnehavare samt driva databasen på ett korrekt, effektivt och robust sätt. Några närmare tekniska kravspecifikationer ställer riktlinjerna inte upp. Konkretiseringsgraden är alltså inte särskilt mycket högre än den i GAC:s principer.

[1] se http://www.icann.org/cctlds/cctldconst-4th-best-practices-10mar01.htm.

II-stiftelsen har enligt dokumentation som överlämnats till utredningen för egen del antagit Best Practice-riktlinjer per den 1 juni 2000. Stiftelsens riktlinjer korresponderar till stor del med de Best Practice-riktlinjer som utarbetats i ICANN:s regi.

I NIC-SE:s verksamhet tillämpas vissa driftregler som gäller infogande, ändrande eller borttagande av DNS-poster kopplade till registrerade domännamn i *se*-zonen. Enligt dessa skall *se*-domänen drivas i enlighet med de RFC:er som definierar standarden för DNS-systemet. Driftreglerna ställer vidare upp vissa krav på DNS-data knutna till domännamn under *se*-domänen. Sådana data för ett domännamn som används för att tekniskt peka ut – delegera – en viss huvuddomän under *se*-domänen, t.ex. poster som anger vilka namnservrar som betjänar huvuddomänen (NS-post), skall anges i *se*-domänen. De skall även anges i zonfilen för den underliggande eller delegerade huvuddomänen dit pekningen sker. Detta medför att den tekniska administratören för huvuddomänen måste anmäla förändringar till den som administrerar *se*-domänen. NS-posterna skall peka ut den underliggande huvuddomänens namnservrar i form av namn, och inte IP-nummer.

De funktionella krav som ställs är bl.a. följande.

- den delegerade zonen skall uppfylla standarden för DNS,
- de utpekade namnservrarna skall antingen motsvaras av giltiga glue-poster, dvs. poster som anger vilken IP-adress som motsvarar ett visst domännamn och som måste finnas med i delegeringen för att den skall fungera, eller vara uppslagbara genom DNS,
- de utpekade namnservrarna skall svara på DNS-frågor och vara auktoritativa för den delegerade zonen,
- de angivna NS-posterna skall ingå i den delegerade zonen i exakt samma form, dock får fler NS-poster ingå i zonen,
- den i SOA-posten, dvs. Start of a Zone of Authority-posten som anger parametrar för och information om zonen, angivna e-postadressen skall gå till den eller de som ansvarar för driften av zonen och är avsedd att läsas av fysiska personer.

II-stiftelsen driver också ett projekt för att formulera en kravspecifikation för drift av DNS. Det bakomliggande syftet med kravspecifikationen är att höja kvaliteten på DNS inom *se*-domänen, men även inom huvuddomänerna under toppdomänen.

Målsättningen är att förbättra tillgängligheten till tjänster inom domäner registrerade under *se*-domänen och vidareutveckla den svenska infrastrukturen för Internet i Sverige. För att kraven skall kunna följas upp avser II-stiftelsen även att utveckla ett verktyg som gör det möjligt för NIC-SE att mäta kvaliteten i *se*-domänens underliggande domäner. I ett därefter kommande steg är avsikten att även erbjuda Internetanvändare i Sverige en funktion för att mäta kvaliteten i den egna domänen och även viss support vad beträffar uppföljning av eventuella brister.

9.3.1.2 Överväganden

Vårt förslag: Lagen bör innehålla de övergripande krav som kan ställas på den tekniska driften av den nationella toppdomänen för Sverige. Det bör även införas en skyldighet för den administrativt ansvarige att följa de nationella föreskrifter som i vederbörlig ordning beslutats inom området. Sådana föreskrifter bör utformas med särskilt beaktande av de riktlinjer om teknisk drift av en nationell toppdomän som ICANN antagit.

Regeringen eller den myndighet regeringen bestämmer bör bemyndigas att meddela sådana tekniska föreskrifter.

Det kan konstateras att varken GAC:s principer eller de övriga dokument som utarbetats – inom IANA, ICANN eller Centr – ställer upp några i nuläget mätbara eller konkretiserade krav på den tekniska driften av en nationell toppdomän. Det råder också vissa svårigheter att närmare precisera sådana. Oaktat detta förhållande har den tekniska driften av den nationella toppdomänen för Sverige utförts på ett väl fungerande sätt. Det kan därför ifrågasättas om det föreligger behov av en offentligrättslig reglering i denna fråga utöver den självreglering som finns. Det samhälleliga intresset av en väl fungerande Internetanvändning är dock stort. Redan detta förhållande medför enligt utredningens mening att det bör ges i vart fall en övergripande reglering i en ny lag om domännamnshantering.

Den nya reglering vi föreslår har enligt sin ändamålsbestämmelse till syfte att säkerställa att administrationen av en nationell toppdomän för Sverige utförs på ett robust, säkert och effektivt sätt i allmänhetens intresse. En på detta sätt formulerad bestämmelse ger möjlighet för tillsynsmyndigheten att utifrån eventuella

internationella eller nationella riktlinjer och dokumentation om bästa teknik m.m. i föreskriftsform kunna säkerställa en väl fungerande teknisk drift av den nationella toppdomänen.

Avsaknaden av tekniska krav samt den oklarhet som synes föreligga om vad som bör gälla i tekniskt hänseende, medför en svårighet att närmare bestämma de tekniska kraven på driften. Starka skäl talar för att överlåta till regeringen eller tillsynsmyndigheten att efter behov och vederbörligt samråd med den lokala Internetgemenskapen, inklusive den administrativt ansvarige, meddela föreskrifter om t.ex. de tekniska konfigurationer som är nödvändiga för att domännamnet skall fungera. Mot denna bakgrund är det lämpligt att införa en reglering av innebörd att den administrativt ansvarige är skyldig att följa de föreskrifter som regeringen eller annan därtill bemyndigad meddelat om tekniska krav på driften. Sådana föreskrifter bör utformas med särskilt beaktande av de riktlinjer som ICANN i förekommande fall har antagit.

9.3.2 Driftsäkerhet

9.3.2.1 Allmänt om säkerhet[2]

Utvecklingen går fortsatt mot en ökad användning av Internet för viktiga samhällsfunktioner. Statsmakterna har därför konstaterat att det är ett samhälleligt intresse att Internet fungerar på ett tillfredsställande och säkert sätt. I prop. 2001/02:158 s. 104, Samhällets säkerhet och beredskap, klargör således regeringen att det är angeläget att samhällsviktiga system har en hög säkerhetsnivå och att insatserna för informationssäkerheten ökas.

Informationssäkerhet syftar till att skydda information främst med avseende på tillgänglighet, kvalitet, sekretess och spårbarhet. Med tillgänglighet avses möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid. Med kvalitet avses att informationen skall vara användbar för en given användare och ett givet problem. I sammanhanget avses med sekretess att innehållet i ett informationsobjekt inte får göras tillgängligt eller avslöjas för obehöriga. Spårbarheten går ut på att verksamheten och

[2] se Informationstekniska standardiseringens (ITS) rapport *Terminologi för informationssäkerhet*, mars 1994, http://www.its.se/its/rapport/ITS6.htm.

tillhörande system skall innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer.

Informationssäkerhet kan delas upp i administrativ säkerhet och teknisk säkerhet. Med *administrativ säkerhet* avses huvudsakligen de administrativa rutiner och procedurer som rör informationshanteringen. *Teknisk säkerhet* kan delas upp i IT-säkerhet och fysisk säkerhet. Vad begreppet *IT-säkerhet* skall anses innefatta är inte helt klart. Sårbarhets- och säkerhetsutredningen har accepterat en definition av begreppet IT-säkerhet i betydelsen skydd av information i informationsbehandlande tekniska system (SOU 2001:41, s. 189). Utredningen godtar denna definition.

IT-säkerhet kan i sin tur delas upp i ADB-säkerhet och kommunikationssäkerhet. Med *ADB-säkerhet* avses säkerhet i form av skydd av data och system mot obehörig åtkomst eller obehörig eller oavsiktlig förändring eller störning vid databehandling. Med *kommunikationssäkerhet* avses säkerhet i samband med överföring av information eller styrsignaler.

Det är tydligt att IT-säkerhet omfattar ett antal vitt skilda funktioner, t.ex. säkerhet beträffande innehållet i och överföringen av information. Vad begreppet IT-säkerhet inte innefattar är *fysisk säkerhet*. Med detta begrepp avses säkerhet i ett systems omgivning avseende byggnads- eller andra tekniska skyddsåtgärder, t.ex. säkerhet för infrastruktur med användande av säkerhetsskåp, inbrottslarm, brandskyddsväggar m.m.

Av det anförda framgår att med säkerhet avses en egenskap eller ett tillstånd som innebär skydd mot okontrollerad insyn, förlust eller påverkan. I IT-sammanhang kan man säga att ett system är säkert i den utsträckning man anser sig kunna lita på dess funktionalitet. Denna bedömning påverkas av de existerande och potentiella hot som man kan se mot systemet.

Med *hot* förstås en möjlig oönskad händelse som ger negativa konsekvenser för en utsatt verksamhet. De hot som kan förekomma mot Internet i stort och dess användning är av skiftande karaktär. De kan delas in i fysiska och logiska hot. Med *fysiska hot* avses t.ex. brister i elförsörjning, brand, översvämning, fysiska intrång, explosioner, avgrävning av kablar m.m. Med *logiska hot* avses t.ex. resursblockering, felaktiga implementationer av IP, programmerade attacker, förfalskning av avsändaradress m.m. Dessa former av hot kan i sin tur delas in i avsiktliga och oavsiktliga hot. Vad som förstås med avsiktliga hot är tämligen klart. Oavsikt-

liga hot kan utgöras av dator- och programvarufel, mänskliga misstag och naturfenomen som åska, brand, översvämning m.m.

Regeringen konstaterar i prop. 2001/02:158 s. 105 att erfarenheter från det säkerhetsarbete som bedrivits av myndigheter och företag avseende IT-relaterade hot, dvs. hot via eller mot informationssystem, visar att den största sårbarheten kan härröras till oavsiktliga hot såsom tekniska fel, bristande planering m.m. Även sårbarheten avseende avsiktliga hot genom egna anställda (s.k. insiders) är stor eftersom möjligheterna för någon inom en organisation att obehörigt föra med sig hemligheter ut eller att förbereda ett system för en attack utifrån är relativt stora.

9.3.2.2 Säkerhet vad gäller DNS

DNS utgör en viktig funktion för att uppnå effektivitet i nätet (jfr bl.a. prop. 1999/2000:86 s. 45). Det är därför av vikt att säkerställa att DNS fungerar på ett robust, säkert och effektivt sätt. Robusthet kan tillskapas genom att tillse att det i systemet finns kapacitet att motstå olika former av attacker däribland DOS-attacker (dvs. Denial of Service-attack som avser en tillgänglighetsförhindrande attack, vanligen utförd genom avsiktlig överbelastning), att den för verksamheten använda utrustningen har en geografisk spridning och organisatorisk spridning med fysiskt skydd, att organisation är utformad på ett sådant sätt att beroenden undviks samt att kompetensen hos driftsorganisationerna är hög.

Korrektheten av informationen i och därmed hela DNS-tjänsten kan äventyras av olika anledningar. En sådan är att den administrativt ansvarige eller av denne anlitat organ, för närvarande NIC-SE, levererar en felaktig zonfil för toppdomänen *se*, dvs. ett utdrag av för adresseringsfunktionen nödvändig information om IP-adresser och domännamn ur toppdomänens originaldatabas. En annan är att extern person manipulerar DNS-data. Så kan ske genom förfaranden i samband med att zonfilen överförs från NIC-SE och *se*-domänens masterserver till toppdomänens slavservrar. Manipulationen av DNS-data kan också ske i användarnas namnserver (resolver), på rotservernivå och på huvuddomänsnivå.

Många har alltså möjlighet att göra behöriga såväl som obehöriga medvetna eller omedvetna ändringar i DNS. Därmed följer ökade risker för förekomst av falska uppgifter i systemet. Falska uppgifter öppnar möjligheter för obehöriga att styra om trafik, avlyssna eller

förvanska information och störa transaktioner. En standard för säker hantering av domännamnsinformation – Secure DNS (DNSSEC) – har därför utvecklats.

För att DNS-tjänsten skall fungera krävs, förutom DNS-operatörer, även medverkan av operatörer som tillhandahåller IP-transport. Vad utredningen har att ta ställning till är dock begränsat till hur robusthet, säkerhet och effektivitet kan uppnås i administrationen av den nationella toppdomänen *se* eller den däri ingående delen av DNS-tjänsten. Övriga delar av DNS-tjänsten, roten och huvuddomänerna, ansvarar andra organ för.

9.3.2.3 Säkerhet i administrationen av *se*-domänen

Namntilldelning och registerföring

Ett kritiskt moment vid registreringen av domännamn är att korrekt information erhålls och lagras i DNS-databasen för den nationella toppdomänen *se*. Ett andra sådant moment utgörs av uppdateringsfunktionen som kräver ett säkert införande av ändringar i databasen så att all information är aktuell och korrekt.

DNS-databasen eller originaldatabasen för toppdomänen *se* handhas för II-stiftelsens räkning av dotterbolaget NIC-SE som en del av uppdraget att sköta den praktiska driften av administrationen av denna. DNS-databasen finns på en server hos NIC-SE och används, bl.a. av säkerhetsskäl, inte för adressöversättning. De delar som behövs för adresseringsverksamheten dras ut ur databasen till en s.k. zonfil som kopieras regelbundet till en operativ original-namnserver. Zonfilen bör innehålla information om vilken IP-adress det är som motsvarar ett efterfrågat domännamn, till vilken värd e-post skall levereras, vilket domännamn som motsvarar en efterfrågad IP-adress, minst en specificerad officiell namnserver för zonen samt parametrar för och information om zonen.

Skulle de inlagda och därefter kopierade uppgifterna vara felaktiga kan kommunikation inte ske till rätt adress. Ett sådant scenario är mycket allvarligt. För att tillförsäkra administrationen en hög säkerhet måste, såsom Domännamnsutredningen funnit, det finnas klara rutiner för verksamheten samt en organisation som har såväl tekniska som personella förutsättningar att klara de krav som administrationen av den nationella toppdomänen *se* kräver. Av

vikt är också att det inom organisationen förekommer kontroll av de personer som skall utföra denna verksamhet.

Redundans i systemet

I sin rapport Är Internet i Sverige robust har PTS konstaterat att DNS-systemet sedan länge har utformats med redundans, dvs. reservkapacitet t.ex. i form av en alternativ anslutningskabel eller dubblerad datorutrustning.

Som ovan redovisats används inte *se*-domänens original- eller kunddatabas i sig för adressöversättning. Zonfilen kopieras ur kunddatabasen till en operativ namnserver eller masterserver. Denna masterserver används i sin tur för vidare kopiering av zonfilen till två distributionspunkter. Dessa utgörs av två namnservrar som av bl.a. redundansskäl är lokaliserade en hos NIC-SE och en hos Netnod. Båda namnservrarna drivs och underhålls av NIC-SE. Från dessa namnservrar hämtas och kopieras informationen om *se*-zonen av bl.a. de för tillfället sju officiella namnservrarna för den nationella toppdomänen *se*. Det är alltså dessa namnservrar – inklusive masterservern – som utnyttjas av användarna på Internet för adressöversättning.

De sju – inom kort åtta - officiella namnservrarna, vanligen kallade slavservrar eller speglande servrar, är placerade på olika platser i syfte att skapa geografisk spridning och därmed minskad sårbarhet. Bl.a. finns sådana hos Netnod, vid KTHNOC, vid Lunds tekniska högskola, hos UUNET i USA (numera MCI) samt hos Skanova (fr.o.m. juni 2003 enligt uppgift från II-stiftelsen).

För att upprätthålla en hög nivå av robusthet i administrationen av toppdomänen *se* bör namnservrar och annan viktig utrustning placeras geografiskt, men även organisatoriskt, skilda från varandra i väl skyddade och underhållna utrymmen, med tillgång till reservkraft m.m. Sålunda har viktig utrustning för DNS-tjänsten placerats i de bergrum som PTS inrättat för telekommunikationer (se prop. 2001/2002:158 s. 101).

Med organisatorisk åtskillnad avses i detta sammanhang att t.ex. driften av namnservrarna i DNS anförtros åt flera uppdragstagare. Tillgängligheten, dvs. möjligheten att uttnyttja resurser efter behov i förväntad utsträckning och inom önskad tid, till för *se*-domänen viktiga namnservrar bör även säkerställas genom tillskapandet av alternativa distributionsvägar. Detta kan uppnås genom att ha flera

olika anslutningar mot Internet och mot olika operatörer. Strävan bör alltså vara att skapa så få beroendeförhållanden som möjligt.

Vidare bör namnservrarna för toppdomänen *se* vara placerade på funktionellt bästa sätt med hänsyn till trafikvolymer m.m. Av vikt är också att namnservrarnas placering inte möjliggör att flera av dem slås ut till följd av enstaka fel eller medför att en större grupp användare inom Sverige inte kan få tillgång till någon *se*-server i Sverige.

Säker hantering av DNS-information

Det är av mycket stor betydelse för funktionen av den nationella toppdomänen *se* att kopieringen eller speglingen av zonfilen för *se*-domänen görs på ett sådant sätt att kopiorna är aktuella och korrekta. Tidigare har konstaterats att det tekniska system som för närvarande används för DNS-tjänsten har vissa säkerhetsbrister (se bl.a. SOU 2000:30 s. 62 f.). Förhållandet beror huvudsakligen på att informationsflödet till och från namnservrarna för *se*-domänen är oskyddat. Domännamnsutredningen förordade användningen av tekniken DNSSEC. Enligt vad som framgått under utredningens arbete pågår alltjämt arbetet med att ta fram den nämnda tekniken för säker DNS även om en övergång dit redan påbörjats.

DNSSEC definierades ursprungligen i RFC 2065, Domain Name System Security Extensions.[3] Dokumentet har dock ersatts av RFC 2535 med samma namn.[4] Tekniken använder DNS för distribution av kryptografiska nycklar och signaturer. I DNSSEC skyddas den känsliga informationen av kryptografiska kontrollsummor. Detta torde innebära att DNSSEC i huvudsak medför säkrare namnuppslagningar, minskad risk för manipulation av information och förfalskade domännamn. Tekniken är därför väl lämpad för att minimera eller avvärja t.ex. attacker som används för att dirigera om webbklienter från en webbplats till en webbplats med t.ex. pornografiskt innehåll. När arbetet med framtagandet av standarden eller tekniken har lett till ett slutresultat torde DNSSEC alltså ge användaren möjlighet att kryptografiskt verifiera om en DNS-uppslagning är korrekt och på så vis kunna upptäcka en attack och vidta nödvändiga åtgärder för att avstyra denna.

[3] se http://www.ietf.org/rfc/rfc2065.txt?number=2065.
[4] se http://www.ietf.org/rfc/rfc2535.txt?number=2535.

Övergången lär dock kräva omfattande tekniska och organisatoriska anpassningar.

Utöver DNSSEC finns även en teknik för att säkra DNS-kommunikationen kallad Transaction Signatures, TSIG. Denna teknik regleras i RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).[5] Den bygger på kryptering av överföringen och innebär att parterna kan använda en gemensam hemlig nyckel för digital signering av DNS-transaktioner och autentisering av trafik – dvs. kontroll av att trafiken kommit fram oförändrad – mellan parter, för zonfilöverföring samt för autentisering vid dynamisk uppdatering av DNS (DDNS).

9.3.2.4 Överväganden

Vårt förslag: Lagen bör innehålla de övergripande driftssäkerhetskrav som kan ställas på driften av den nationella toppdomänen för Sverige. Det bör även införas en skyldighet för den administrativt ansvarige att följa de nationella föreskrifter som i vederbörlig ordning beslutats inom området. Sådana föreskrifter bör utformas med särskilt beaktande av de riktlinjer för säkerhet vid drift av en nationell toppdomän som ICANN antagit.

Regeringen eller den myndighet regeringen bestämmer bör bemyndigas att meddela sådana föreskrifter.

I GAC:s principer föreskrivs inte närmare vad den administrativt ansvarige faktiskt skall göra såvitt gäller upprätthållande av en robust och säker administration av en nationell toppdomän. Vissa generella bestämmelser av betydelse ger principerna dock, t.ex. i artikel 10 som avser att reglera förhållandet mellan ICANN och den administrativt ansvarige.

Av artikel 10.2.1 i GAC:s principer följer att den administrativt ansvarige för en nationell toppdomän skall ombesörja att de auktoritativa eller officiella master- och slavnamnservrarna för toppdomänen hanteras och vidmakthålls på ett stabilt och säkert vis. Vidare skall den administrativt ansvarige tillse bl.a. att zonfilen för den nationella toppdomänen samt riktiga och uppdaterade registreringsuppgifter fortlöpande hålls tillgängliga för att trygga den nationella toppdomänens driftstabilitet.

[5] se http://www.ietf.org/rfc/rfc2845.txt?number=2845.

Enligt artikel 10.2.3 skall den administrativt ansvarige trygga säkerheten och integriteten av innehållet i registerdatabasen. Med integritet torde avses förmågan att upprätthålla ett värde genom skydd mot oönskad förändring, påverkan eller insyn. I uppgiften ligger att bestämma riktlinjer för datadeposition eller för speglingsplats för registrerade data som handhas av denne. Bestämmelsen knyter an till det ovan förda resonemanget om tillförlitligheten av den information som namnservrarna skall innehålla.

Artikel 10.2.5 ålägger den administrativt ansvarige en skyldighet att följa ICANN:s riktlinjer i olika frågor, t.ex. om samverkansförmåga mellan en nationell toppdomän och andra delar av DNS och Internet samt erhållande och vidmakthållande av och tillträde för allmänheten till riktig och uppdaterad kontaktinformation avseende personer som registrerar domännamn.

Med införandet i en ny lag av en ändamålsbestämmelse av innebörd att administrationen av en nationell toppdomän skall utföras på ett robust, säkert och effektivt sätt i allmänhetens intresse, ges den övergripande ramen för verksamheten i driftsäkerhetshänseende. Att närmare ange vilka specifika åtgärder som skall vidtas för att säkerställa driftsäkerhet kan medföra föreskrifter med utförliga tekniska specifikationer m.m. Ett införande i lag av på så sätt utformade bestämmelser låter sig inte lämpligen göras enligt svensk lagstiftningstradition. Det finns också möjlighet för att bättre teknik kan utvecklas och en lagreglerad skyldighet att upprätthålla visst säkerhetsskydd på ett angivet sätt kan därför medföra en tung och tidskrävande införandeprocess.

För att skapa vissa närmare kriterier för verksamheten bör dock lagen innehålla skyldighet för den administrativt ansvarige att säkerställa att en nationell toppdomän – inom rimliga gränser och med användande av bästa kända teknik – skyddas från såväl fysiska som logiska hot och att säkerhetskopior görs av registreringsdata nödvändiga för en fungerande och effektiv adressering på Internet. Det finns därutöver skäl att låta regeringen eller den myndighet regeringen bestämmer meddela nödvändiga kompletterande föreskrifter på detta område. Därvid bör särskilt beaktas de riktlinjer för verksamheten som utarbetas av ICANN.

9.3.3 Ett offentligt register avseende kontaktinformation

I samband och som ett led i administrationen av en nationell toppdomän erhålls en mängd uppgifter som på något sätt måste systematiseras i ett register. Detta sker till stor del genom namntilldelningsförfarandet under vilket informationen antecknas i ett register i en databas. I registret införs bl.a. uppgifter om det registrerade domännamnet, vilka namnservrar som betjänar domännamnet, kontaktuppgifter till den tekniska administratören hos domännamnsinnehavaren och de övriga tekniska uppgifter som behövs för att upprätthålla domännamnet. En viktig uppgift är att hålla registret uppdaterat och tillse att informationen i det är korrekt. Den aktuella kunddatabasen används därefter såväl i den tekniska driften av toppdomänen för domännamnsuppslagning som i den administrativa verksamheten med namntilldelning.

9.3.3.1 Den s.k. who is-tjänsten

GAC:s principer föreskriver i artikel 9.1.7 att staten bör tillse att den administrativt ansvarige för en nationell toppdomän för Sverige följer de riktlinjer som ICANN har utarbetat för verksamheten. De riktlinjer som avses omfattar enligt artikel 10.2.5 bl.a. riktlinjer för erhållande och vidmakthållande av samt tillträde för allmänheten till riktig och uppdaterad kontaktinformation avseende personer som registrerar domännamn.

Den kontaktinformation som bör finnas i ett register tillgängligt för allmänheten tillhandahålls redan på frivillig väg i dag genom den s.k. who is-tjänst som kan nås via NIC-SE:s webbplats. [6] Who is-tjänsten utgörs av en sökbar registerfunktion där uppgifter kan erhållas om vem som innehar ett domännamn, dennes offentliga kontaktuppgifter huvudsakligen i form av adressuppgifter, uppgifter om de namnservrar som betjänar domännamnet, var den tekniska administratören hos domännamnsinnehavaren kan nås samt övriga tekniska uppgifter som behövs för att upprätthålla domännamnet.

[6] se http://www.nic-se.se/domaner/domansok.shtml.

9.3.3.2 Överväganden

Vårt förslag: Lagen skall innehålla en skyldighet för den administrativt ansvarige att tillhandahålla ett allmänt tillgängligt register med kontaktinformation m.m. Domännamnsinnehavare skall låta registrera sitt domännamn och kontaktinformation i det nämnda centrala registret för vilket den administrativt ansvarige för en nationell toppdomän för Sverige är registeransvarig.

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om registerverksamheten.

Registret får användas för att fastställa vem som är innehavare till en huvuddomän samt för att i övrigt vid behov kunna komma i kontakt med domännamnsinnehavaren eller dennes företrädare.

Det register som nu avses skall enligt GAC:s principer vara allmänt tillgängligt. Med hänsyn till att driften av registret enligt vårt förslag kan utföras av ett privaträttsligt organ måste en reglering i detta hänseende komma till stånd för att så med säkerhet skall bli fallet.

En väg att gå för att göra registret allmänt tillgängligt är att göra tryckfrihetsförordningens regler om allmänna handlingar tillämpliga på registret. Detta kan ske genom att organet och dess registerverksamhet anges i den bilaga som avses i 1 kap. 8 § andra stycket sekretesslagen (1980:100). En annan väg att gå är att, såsom utredningen föreslagit i EkomL, i lag ange att registret skall hållas allmänt tillgängligt samt överlåta till regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten att meddela de närmare föreskrifterna för hur detta skall gå till och vad registret skall innehålla.

I enlighet med vad som konstaterats ovan i kapitel 6 skall personuppgiftslagen (1998:204), PUL, tillämpas på ett register med kontaktinformation eftersom detta innehåller personuppgifter. Enligt PUL får personuppgifter endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får sedan inte behandlas för något ändamål som inte är förenligt med det ursprungliga. De personuppgifter som behandlas skall dessutom vara adekvata och relevanta i förhållande till ändamålet. Fler uppgifter än som är nödvändiga med hänsyn till ändamålet får inte behandlas. Av vikt är att de personuppgifter som behandlas är riktiga och aktuella. Alla rimliga åtgärder skall vidtas för att rätta, blockera

eller utplåna felaktiga eller ofullständiga uppgifter. PUL är subsidiär i förhållande till annan lag eller förordning.

De krav som GAC:s principer ställer upp på registrets korrekthet vad gäller information m.m. följer till stor del redan av PUL. Det kan mot bakgrund av det anförda ifrågasättas om det, utöver säkerställandet att registret blir allmänt tillgängligt, behövs en ytterligare reglering av registerverksamheten i en ny lag. Det finns inte heller några bestämmelser om när behandling av personregister bör regleras i en särförfattning. Saken får avgöras från fall till fall.

Svensk rätt ställer inte upp krav på att regler om registrering skall ges i lagform (jfr 8 kap. 2 och 3 §§ regeringsformen). Regeringen har dock tidigare uttalat (se prop. 1990/91:60 s. 58 och prop. 1997/98:44 s. 41) att en målsättning bör – för det fall att register eller reglering av register skall införas – vara att bestämmelserna meddelas i form av lag. Detta gäller om det t.ex. inrättas register med ett stort antal registrerade och ett särskilt känsligt innehåll och i de fall uppgifterna i registret sprids externt i en icke obetydlig omfattning. Allmänt kan alltså sägas att en särreglering kan vara motiverad t.ex. när behandlingen omfattar personuppgifter om hela befolkningen eller en stor del av denna eller när det rör sig om känsliga personuppgifter.

Det nu aktuella registret kan inte sägas vara av sådant känsligt slag att eventuella bestämmelser behöver finnas i lag. Det register som nu avses kommer med hänsyn till den ökande registreringen av domännamn under den nationella toppdomänen *se* att omfatta allt fler personer. Tillväxten har under senare år uppgått till cirka 15 000 domännamn per år.[7] Vid årsskiftet fanns det cirka 103 000 delegerade domäner under *se*-domänen.[8] Under innevarande år har, med övergången till det nya regelverket för namntilldelning, cirka 50 000 nya domännamn registrerats. Detta förhållande utgör dock, som utredningen ser det, en engångsföreteelse och ökningen kan inte tas till intäkt för en dramatisk ökning av domännamnsregistreringen i framtiden. Med hänsyn härtill och till att varje domännamnsregistrering i sig inte motsvarar en personuppgift – flera domännamnsinnehavare kan ha samma kontaktinformation – torde omfattningen av personuppgifter inte i sig omfatta så stor del av befolkningen att det redan på denna grund bör införas en lagreglering av registerverksamheten.

[7] se http://www.nic-se.se/domaner/tillvaxt.shtml.
[8] se Simon Josefsson datakonsult, http://josefsson.org/dns/.

Förhållandet att registret med kontaktinformation skall vara allmänt tillgängligt sammantaget med syftet bakom who is-tjänsten kan däremot medföra att uppgifterna i registret sprids externt i en icke obetydlig omfattning. Det kan därför finnas skäl att av denna anledning i lag reglera registerverksamheten.

Att föra ett register av ifrågavarande slag kräver utrustning men framför allt ett noggrant och systematiskt förfarande för att säkerställa att registret hela tiden är uppdaterat med korrekta uppgifter. För att finansiera registerverksamheten är det därför tänkbart att en avgift skall få tas ut. En eventuell sådan avgift bör täcka kostnaderna för registreringen. I dag tar den administrativt ansvarige ut en årsavgift för innehavet av ett domännamn. Denna avgift är som utredningen ser det tillfyllest för att säkerställa finansieringen av den aktuella registreringsverksamheten m.m.

Närmare föreskrifter om registreringen, registret och eventuella avgifter bör meddelas av regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten.

9.4 Särskilt om hur namntilldelningen bör regleras

9.4.1 Inledning

Vårt lagförslag innebär att samtliga de åtgärder som genomförs inom ramen för administrationen av toppdomänen skall uppfylla vissa generella krav. Det bör emellertid diskuteras om denna typ av reglering är tillräcklig för den del av administrationen som avser namntilldelning och, om så inte kan sägas vara fallet, hur en eventuell ytterligare reglering bör utformas.

För att kunna diskutera frågorna om regelverket för namntilldelning kommer vi i detta kapitel att redovisa vilka olika regler som brukar gälla för olika toppdomäner och hur det svenska regelverket är utformat.

9.4.2 Olika metoder att fördela domännamn

Den som ansöker om att få registrera ett domännamn under en toppdomän måste i allmänhet uppfylla vissa krav. Vilka krav som uppställs varierar från toppdomän till toppdomän. Man kan här skilja mellan regelsystem som innehåller bestämmelser om förprövning och regelsystem som saknar sådana bestämmelser.

Systemen med förprövning går i de flesta fall ut på att den som vill registrera ett domännamn måste kunna visa på någon form av namntillhörighet. För att en ansökan om registrering skall beviljas kan sökanden exempelvis vara tvungen att uppvisa en firma- eller varumärkesregistrering eller en registrerad rätt till ett varumärke. I ett system utan förprövning förekommer ingen kontroll innan registreringen beviljas. Att en toppdomän saknar bestämmelser om förprövning innebär emellertid inte att systemet saknar regler i fråga om de registrerade domännamnen. Om det efter att ett domännamn registrerats kan konstateras att domännamns-innehavaren inte följer gällande regler för domänen kan domännamnet vanligtvis avregistreras. Domännamnsutredningen har i sitt betänkande .se? (SOU 2000:30) i en jämförelse mellan system med och system utan regler om förprövning konstaterat att de toppdomäner där förprövning saknas oftast har fler registrerade domännamn.[9] Exempelvis hade den danska nationella toppdomänen *dk*, där det inte sker någon förprövning, dubbelt så många registreringar jämfört med det tidigare svenska systemet med förprövning.

Regelverk för namntilldelning med förprövning förekommer nästan enbart beträffande vissa nationella toppdomäner. Namntilldelning under de generiska toppdomänerna sker vanligen utan sådan prövning.

9.4.3 Det svenska regelsystemet

Som nämnts ovan trädde ett nytt regelverk för namntilldelning under toppdomänen *se* i kraft i början av april 2003. De nya reglerna gör det möjligt för fysiska och juridiska personer att registrera domännamn under toppdomänen *se*. För utländska juridiska personer utan fast driftställe i Sverige eller för fysiska personer utan stadigvarande hemvist i Sverige gäller att sökanden måste uppge en kontaktperson med stadigvarande hemvist i landet. Detta bl.a. för att det skall vara möjligt för NIC-SE att nå innehavaren av domännamnet med meddelanden och fakturor.

Vid tilldelningen av domännamn tillämpas vad som i II-stiftelsens regler kallas "först till kvarn"-principen, dvs. att registreringen av domännamn sker i den ordning som ansökningarna kommer in. Regelverket ger bara i vissa mycket begrän-

[9] Se SOU 2000:30 s. 31

sade fall möjlighet till att reservera domännamn. Denna möjlighet är bl.a. förbehållen kommuner i fråga om kommunnamn. Regelsystemet ger däremot inga möjligheter till förtur till domännamn.

Domännamn skall, liksom vad som gällde i det tidigare tillämpade regelsystemet, innehålla bokstäverna A–Z eller siffrorna 0–9. Det är också möjligt att använda bindestreck i ett domännamn. Domännamnet måste inledas eller avslutas med en bokstav eller siffra och får inte uteslutande bestå av siffror. Det domännamn som ansökan avser får innehålla lägst två tecken och högst 63 tecken.

Innehavaren av ett domännamn under toppdomänen *se* har ensamrätt till detta under domänen under den tid som registreringen avser. Ett domännamn som registrerats utgör därmed hinder för att ett identiskt domännamn registreras under toppdomänen. Ett domännamn kan inte heller registreras om det utgör en underdomän till ett redan registrerat domännamn. Däremot kan innehavaren av ett domännamn också registrera domännamn under de underdomäner som NIC-SE tillhandahåller.

Om förutsättningarna för registrering är uppfyllda, skall domännamnet registreras i enlighet med ansökan. Ett registrerat domännamn kan dock avregistreras i en rad fall.

De grunder för avregistrering som nämns inledningsvis i regelsystemet rör de fall där innehavaren av ett domännamn inte uppfyller de skyldigheter som åligger denne. Avregistrering kan sålunda ske om innehavaren inte lämnar fullständiga och korrekta uppgifter till NIC-SE eller underlåter att underrätta bolaget om att uppgifterna inte längre är korrekta, om en eventuell kontaktperson inte lämnat samtycke till att dennes personuppgifter behandlas i enlighet med personuppgiftslagen (1998:204) eller om innehavaren av ett domännamn inte betalar den överenskomna årsavgiften. En annan grund för avregistrering är att innehavaren inte lämnat en e-postadress där innehavaren själv eller en kontaktperson kan nås av NIC-SE. Slutligen kan avregistrering ske, vad gäller den här aktuella kategorin av grunder, om det registrerade domännamnet uppenbart strider mot svensk lag eller författning. Innan ett domännamn avregistreras skall innehavaren, förutom i det sistnämnda fallet, beredas möjlighet att avhjälpa den brist som kan föranleda åtgärden från NIC-SE:s sida.

Avregistrering kan också ske på grund av att svensk domstol i laga kraft vunnen dom eller beslut med rättskraft konstaterat att avregistrering skall ske.

NIC-SE har också rätt att avregistrera ett domännamn eller överföra ett domännamn till annan innehavare om detta beslutas efter genomförandet av ett alternativt tvisteförfarande. Detta under förutsättning att inte innehavaren visar att denne inom viss tid väckt talan vid domstol om rätten till namnet.

Avregistrering kan slutligen också ske efter begäran av innehavaren själv.

9.4.4 Överväganden

Vårt förslag: I lagförslaget bör införas en bestämmelse som anger de övergripande krav som bör ställas på den del av administrationen som rör namntilldelning. Dessa krav bör vara att namntilldelningen skall skötas på ett sätt som är öppet för insyn, icke-diskriminerande och som värnar skyddet för den personliga integriteten. Därtill skall regelverket utformas på ett sätt som beaktar användarnas och andra allmänna intressen samt utvecklingen på Internetområdet. Därutöver föreslår vi en bestämmelse som innebär att ansöknings- och årsavgifter som utgår i anledning av att man ansöker om eller beviljats ett domännamn skall vara skäliga.

Den övergripande målsättningen för den nationella toppdomänen *se* är, som den formuleras i 1 § i vårt lagförslag, att administrationen av toppdomänen skall tillgodose allmänhetens intressen. Detta övergripande krav kan preciseras närmare för var och en av de verksamhetsgrenar som ingår i administrationen. Som redogjorts för i kapitel 5 omfattar den verksamhetsgren som avser tilldelning av domännamn samtliga de åtgärder som möjliggör för en sökande att registrera ett domännamn under toppdomänen. Således utgör mottagandet, handläggningen och registreringen av uppgifter i anledning av ansökan i databasen verksamhet som faller in under begreppet namntilldelning. I denna del av verksamheten bör också ingå utarbetandet och tillämpningen av regelverket för tilldelning av domännamn. Slutligen ingår också bestämmande av avgifter, fakturering och andra liknande åtgärder som vidtas i anledning av att ett domännamn registrerats.

Enligt vad utredningen erfarit fungerar den del av verksamheten som rör namntilldelningen hos NIC-SE väl. Tilldelningen av domännamn sker utifrån klart formulerade regler och det föreligger inga längre väntetider för att få en ansökan behandlad. Vad gäller

det regelverk som används sedan i början av april 2003 medger detta dessutom betydligt större möjligheter att registrera namn under toppdomänen *se* än vad som tidigare varit fallet, vilket ligger väl i linje med det generella kravet att administrationen skall tillgodose allmänhetens intressen.

Trots det här sagda bör det framhållas att införandet av ett regelverk utan förprövning i sig kan medföra vissa nackdelar för tilldelningen av domännamn. Eftersom det nuvarande regelverket ger möjligheter till registrering i annan omfattning än tidigare kan exempelvis en eller flera innehavare registrera ett stort antal domännamn som inte används aktivt. Detta skulle i sig kunna medföra att antalet registreringar ökar, utan att den aktiva användningen av domännamn under toppdomänen ökar. Dessutom kan det ökade antalet ansökningar innebära längre väntetider om man inte kontinuerligt anpassar rutiner och personella resurser. Det nu gällande systemet har vid tidpunkten för överlämnandet av detta betänkande bara varit i bruk under några månaders tid. Det är därför ännu för tidigt att diskutera om de nackdelar med systemet som skulle kunna finnas i teorin också kommer att visa sig i praktiken.

För att framdeles kunna garantera att verksamheten i den del som rör tilldelning av domännamn följer samma huvudsakligen positiva utvecklingslinjer som hittills varit fallet, bör det i en ny lag finnas en bestämmelse som särskilt avser namntilldelningen. Bestämmelsen bör närmare ange de krav som bör ställas för att den delen av verksamheten skall kunna sägas tillgodose allmänhetens intressen. Kraven som bör komma till uttryck i bestämmelsen bör garantera att namntilldelningen sker på ett icke-diskriminerande sätt som ger möjlighet till insyn. Genom att namntilldelningsverksamhet sker på ett sätt som ger möjlighet till insyn ges domännamnsinnehavarna och andra användare möjlighet att reagera om namntilldelning inte längre motsvarar de krav som bör kunna ställas. Därtill bör det av bestämmelsen framgå att reglerna för tilldelning av domännamn skall utformas på ett sätt som beaktar användarnas och andraintressen samt utvecklingen på Internetområdet.

En omständighet som påverkar antalet registreringar under en toppdomän är de kostnader som den som ansöker om en registrering får betala. För att motverka en utveckling där kostnaderna för ett domännamn hämmar utvecklingen av en toppdomän har man i Europaparlamentets och rådets förordning (EG)

nr 733/2002 av den 22 april 2002 om inrättande av toppdomänen .eu valt att införa en bestämmelse som styr vilken avgift som den ansvarige för toppdomänen får ta ut. Detta genom att det i artikel 4 punkten 2 c) sägs att avgiften skall vara direkt baserad på de kostnader som uppstår. Vad detta närmare innefattar framgår inte av förordningen. Bestämmelsens utformning talar emellertid för att avgiften skall bestämmas utifrån de kostnader som kan uppkomma för att driva den verksamhet som administrationen utgör.

Som nämnts ovan bör regelverket för namntilldelningen främja att så många som möjligt skall kunna registrera domännamn under toppdomänen *se*. För att kunna administrera toppdomänen i enlighet med denna målsättning och för att säkra mot en överprissättning bör det i linje med förordningen om *eu* införas en bestämmelse som ger möjlighet att övervaka de avgifter som utgår i anledning av att man registrerar ett domännamn. En sådan bestämmelse bör föreskriva att ansöknings- och årsavgifterna skall vara skäliga.

Med att avgifterna skall vara skäliga menas att de inte får vara av sådan storlek att de kan anses hindra eller försvåra för envar, som så önskar, att få ett domännamn registrerat under den nationella toppdomänen.[10]

9.5 Särskilt om hur tvistlösning bör regleras

Som sagts i kapitel 5 anser vi att tvistlösningsförfarandet bör regleras i lag. För att tillförsäkra att den nationellt ansvarige tillhandahåller ett alternativt tvistlösningsförfarande bör det införas en bestämmelse i lagförslaget som innebär en skyldighet för denne att tillhandahålla ett sådant system. Frågan är emellertid om bestämmelsen också bör ange de övergripande riktlinjer som skall vara vägledande vid utformningen av ett sådant förfarande.

Som bakgrund redovisar vi vad som gäller allmänt om tvistlösningsförfaranden och domännamn och vilken inställning ICANN har beträffande tvistlösningsförfarandenas utformning.

Sedan april 2003 har II-stiftelsen tillhandahållit ett alternativt tvistlösningsförfarande. Detta förfarande beskrivs nedan.

[10] I detta sammanhang bör också nämnas Kommissionens Green paper on services of general interest, 21.052003.COM(2003) 270 final.

9.5.1 Allmänt om tvistlösning och domännamn

Frågan om det finns behov av särskilda alternativa tvistlösningsförfaranden och hur sådana förfaranden bör utformas har diskuterats inom ett flertal internationella organisationer och i en rad länder.

Det tongivande organet i frågor om tvistlösning inom detta och närliggande områden är World Intellectual Property Organisation (WIPO). I april 1999 publicerade WIPO rapporten Report on the First WIPO Internet Domain Name Process, om tvistlösning angående tvister i frågor som rör varumärken och domännamn. De förslag som lades fram i rapporten har i stora delar accepterats av ICANN och återfinns i Uniform Dispute Resolution Policy (UDRP) som är ett tvistlösningssystem för domännamnskonflikter. UDRP är främst inriktat på att hantera konflikter beträffande de toppdomäner som inte har direkt nationell anknytning. De tvistlösningsorgan som prövar tvisterna har därmed inte någon större kunskap eller anledning att ta hänsyn till de nationella förhållandena i de länder som berörs av tvisten. I anledning härav har systemet utsatts för kritik. UDRP används för närvarande främst för konflikter i samband med registrering av domännamn under de generiska toppdomänerna. Trots UDRP:s utformning har emellertid också vissa nationella toppdomäner med kommersiell inriktning kommit att använda sig av systemet. För närvarande pågår ett arbete med att anpassa UDRP på ett sätt som gör systemet lättare att använda också vid konflikter i samband med registrering av domännamn under de nationella toppdomänerna.

För att en tvist skall kunna behandlas efter de regler som UDRP föreskriver krävs att tre förutsättningar är uppfyllda, domännamnet måste vara identiskt eller ägnat att förväxlas med klagandens, innehavaren av domännamnet skall inte ha någon legitim rätt till namnet och domännamnet skall ha registrerats och använts i ond tro.

UDRP administreras av fyra olika tvistlösningsorgan, nämligen CPR Institute for Dispute Resolution, eResolution, The National Arbitration Forum och WIPO Arbitration and Mediation Center. Den som vill anhängiggöra ett ärende kan på egen hand välja vilket av de fyra tvistlösningsorganen som skall pröva tvisten. Prövningen sker av en eller tre personer som utses av det aktuella tvistlösningsorganet. Det beslut som fattas inom ramen för UDRP verkställs av ICANN efter tio dagar. Under denna tid har parterna i tvisten rätt att anhängiggöra tvisten vid domstol.

WIPO har också tagit fram en andra rapport. Denna tar sikte på registrerade domännamn som får anses göra intrång i bl.a. personliga namn, annans firma och namn på internationella organisationer. Det pågår också ett arbete som syftar till att klarlägga inom vilka områden UDRP bör vara tillämplig.

Samtidigt med de här nämnda processerna pågår ett arbete inom WIPO att ta fram ett förslag till ett "ccTLD-program" som innebär att man bistår de nationellt ansvariga för de nationella toppdomänerna med att ta fram regler för att förebygga konflikter om immateriella rättigheter. Programmet innebär också att de nationellt ansvariga skall erbjudas alternativa tvistlösningsformer som är mer effektiva och billigare än ett domstolsförfarande. I detta sammanhang ställs WIPO Arbitration and Mediation Center till de nationellt ansvarigas förfogande om det finns önskemål om detta.

Frågan om hur tvistlösningsförfaranden i anledning av tvister kring registrerade domännamn skall hanteras berörs också kort i RFC 1591 genom att det i artikel 4.1. sägs att när det uppstår en konflikt om rätten till ett särskilt domännamn skall "the registration authority" bara bistå parterna med kontaktinformation. I övrigt skall "the registration authority" varken delta i konfliktens lösande eller ha något ansvar i sammanhanget. I ICP-I berörs frågan genom en hänvisning till vad som sägs i RFC 1591. Det är inte alldeles givet vilken betydelse som nu nämnda uttalanden skall tillmätas. Begreppet "registration authority" används inte i dokumentet i övrigt och av kontexten framgår inte om bestämmelsen avser den som ansvarar för en nationell toppdomän eller annat rättssubjekt som utför den praktiska administrationen.

Också i GAC:s principer berörs frågan om tvistlösning genom att det sägs dels att den som ansvarar för en nationell toppdomän skall tillämpa tvistlösningsförfaranden som säkerställer att alla de registrerades intressen tillvaratas, dels att tvistlösningen i största möjligaste mån bör följa vanliga principer. Hur tvistlösningsförfarandena mer i detalj bör utformas anges inte i principerna. Däremot sägs att utformningen av tvistlösningsproceduren inte får innebära att parterna förtas möjligheten att få frågan prövad i domstol.

9.5.2 II-stiftelsens alternativa tvistförfarande

I II-stiftelsens redogörelse för det alternativa tvistförfarandet anges att syftet med förfarandet är att kunna avgöra enkla tvister på ett snabbt och billigt sätt. En annan bakomliggande tanke anges vara att tvistlösningsproceduren skall ha en förebyggande effekt genom att avhålla från missbruk av kännetecken vid registrering av domännamn.

Det alternativa tvistlösningsförfarandet är avsett att tillämpas vid klara fall av missbruk där innehavaren inte har någon rätt till eller berättigat intresse av den benämning som utgör domännamnet. För att tvistlösningsförfarandet skall vara tillämpligt krävs därutöver att domännamnet skall ha registrerats eller använts i ond tro. Exempel på situationer där så kan sägas vara fallet är bl.a. registreringar av domännamn som syftar till att domännamnet skall säljas eller registreringar av domännamn som syftar till att störa affärsverksamheten för en konkurrent. Att registrera annans varumärke, firma, släktnamn eller liknande utgör exempel på situationer där innehavaren inte kan anses ha rätt till eller berättigat intresse av domännamnet.

En prövning av en registrering av ett domännamn enligt det alternativa tvistlösningsförfarandet resulterar i att innehavaren av domännamnet inte längre har rätt att använda detta. Domännamnet kan därmed också, på sätt som vi beskrivit i kapitel 8.2.2, avregistreras eller överflyttas enligt de allmänna villkor som gäller för namntilldelningen inom NIC-SE. Den som godkänner de allmänna villkoren om namntilldelning anses också ha godkänt att domännamnet kan komma att prövas i det här beskrivna tvistlösningsförfarandet.

Frågor som tas upp till prövning inom ramen för det alternativa tvistlösningsförfarandet skall prövas av en eller tre jurister. De jurister som kan komma i fråga för uppdrag som tvistlösare är sådana som anmält sig till II-stiftelsen och som stiftelsen därefter förtecknat på en lista. Huvudregeln är att tvisten avgörs av en jurist. Det åligger stiftelsen att välja den jurist som skall vara tvistlösare från listan. Om frågan prövas av tre jurister skall parterna utse vardera en jurist och den tredje juristen skall föreslås av II-stiftelsen.

För att få en fråga prövad i det alternativa tvistlösningsförfarandet krävs att man vänder sig till II-stiftelsen genom NIC-SE. Anmälan om att det skall inledas ett tvistlösningsförfarande

skall göras skriftligen. Efter det att anmälan getts in skall denna kommuniceras med motparten. Stiftelsen har därefter att avgöra om det krävs ytterligare skriftväxling.

Vid ansökan om att inleda ett alternativt tvistförfarande utgår en ansökningsavgift om 10 000 kr. I de fall där en tvist avgörs av tre jurister utgår ytterligare en avgift om 10 000 kr. Om tvisten utfaller till fördel för den som inlett förfarandet återbetalas hälften av avgiften.

Trots att det alternativa tvistlösningssystemet i första hand är knutet till det regelverk som trädde i kraft den 2 april 2003 kan också domännamn som registrerats före denna tidpunkt prövas enligt förfarandet.

9.5.3 Överväganden

Vårt förslag: I lagförslaget bör införas en bestämmelse som föreskriver att den som är ansvarig för den nationella toppdomänen skall tillhandahålla ett särskilt förfarande för avregistrering och överföring av domännamn i vissa särskilda fall. Av bestämmelsen skall framgå att förfarandet skall avse frågor om avregistrering och överföring av domännamn vid uppenbara fall av missbruk där innehavaren i ond tro registrerat eller använt ett domännamn och där denne inte har någon rätt till eller berättigat intresse av den benämning som utgör domännamnet. Den som är administrativt ansvarig för den nationella toppdomänen får ta ut en skälig avgift vid behandling av en ansökan om avregistrering eller överföring i de fall som omfattas av den här föreslagna bestämmelsen.

Den rekommendation som återfinns i GAC:s riktlinjer artikel 9.1.6 bör återspeglas i lagförslaget om en ny lag om administrationen av den nationella toppdomänen för Sverige. Lagen bör alltså innehålla ett förpliktande för den som ansvarar nationellt att tillhandahålla ett alternativt tvistlösningsförfarande. Vi väljer att reglera detta genom att föreslå en skyldighet för den administrativt ansvarige att tillhandahålla ett förfarande för avregistrering och överföring av domännamn i vissa särskilda fall.

Den förpliktelse att tillhandahålla ett förfarande för avregistrering och överföring av domännamn i vissa särskilda fall som vi föreslår bör vara avsett att tillämpas på samma slags tvister som det alternativa tvistförfarande som II-stiftelsen tillhandahåller i dag,

dvs. uppenbara fall av missbruk där innehavaren i ond tro registrerat eller använt ett domännamn och där denne inte har någon rätt till eller berättigat intresse av den benämning som utgör domännamnet. Förfarandet för avregistering- och överföring av domännamn i vissa fall bör alltså ersätta det alternativa tvistlösningsförfarandet. Detta innebär att avregistrerings- och överföringsförfarandet kommer att utgöra en överprövning av ett begränsat antal beslut om registrering som fattas i samband med handläggningen av en ansökan. Det bör i detta sammanhang nämnas att det också finns andra grunder för t.ex. avregistrering såsom utebliven betalning av årsavgift som kan leda till att ett domännamn avregistreras. Sådana fall skall fortfarande handläggas av NIC-SE.

Att en fråga om avregistrering avgörs inom ramen för det här beskrivna förfarandet utgör inte hinder för att samma fråga också prövas i en domstolsprocess. Mer komplicerade tvister bör däremot prövas uteslutande av domstol eller enligt lagen (1999:116) om skiljeförfarande.

Ett avregistrerings- och överföringsförfarande av den begränsade karaktär som det här bör uppfylla vissa allmänna förutsättningar. Avregistrerings- och överföringsförfarandet bör sålunda vara snabbt, enkelt, öppet för insyn och medföra en så låg kostnad som möjligt för de som är parter i tvisten. Det bör också krävas att förfarandet genomförs på ett sätt som skapar förtroende för förfarandet. För att kunna garantera att så är fallet bör vissa av de övergripande förutsättningarna komma till uttryck i den lagbestämmelse som reglerar skyldigheten att tillhandhålla ett förfarande för avregistrering och överföring av domännamn i vissa särskilda fall.

Det alternativa tvistlösningsförfarande som nu tillhandahålls inom II-stiftelsens verksamhet bör kunna tjäna som förebild för det här föreslagna förfarandet. II-stiftelsens alternativa tvistlösningsförfarande kan emellertid kritiseras i ett avseende utifrån de ovan nämnda generella kraven. Det gäller den avgift om 10 000 kr som utgår vid anhängiggörandet av en tvist. I och med att det nuvarande regelverket trädde i kraft har det i större utsträckning än tidigare blivit möjligt för privatpersoner att registrera domännamn under toppdomänen. Detta innebär att det kan uppstå fler tvister med enskilda som part som omfattas av tillämpningsområdet för det förfarande som vi föreslår än vad som tidigare varit fallet. En avgift om 10 000 kr utgör ett ansenligt belopp för en enskild. Ett förfarandet med en sådan utformning riskerar därför

att leda till att enskilda väljer att avstå från att utnyttja detta. En avgift om 1 000 kr för juridiska personer och 500 kr för privatpersonerna framstår enligt utredningen i dagsläget som en rimlig avgift. Avgiften bör dessutom vara densamma oavsett om tvisten avgörs av en eller tre ledamöter.

Om II-stiftelsen inte anser det vara möjligt att driva ett avregistrerings- och överflyttningsförfarande som liknar det i dag tillämpade alternativa tvistlösningsförfarandet till denna lägre kostnad för sökanden bör stiftelsen, eventuellt i samråd med tillsynsmyndigheten, omarbeta proceduren. Ett sådant omarbetat förslag bör remissbehandlas och finnas tillgängligt på II-stiftelsens webbplats för synpunkter från allmänheten.

9.6 Särskilt om hur tillsynsverksamhet bör regleras

Vårt förslag: Den myndighet som regeringen bestämmer skall ha tillsyn över efterlevnaden av lagen och de föreskrifter som meddelats med stöd av lagen.

Tillsynsmyndigheten skall inom ramen för tillsynen kunna kräva in information, beredas tillträde till områden, lokaler och andra utrymmen samt meddela förelägganden.

Lagen bör innehålla regler om verkställighet av myndighetsbeslut i enlighet med gällande rätt.

I lagen skall införas en bestämmelse som ger regeringen eller tillsynsmyndigheten bemyndigande att föreskriva om skyldighet för den administrativt ansvarige att betala avgift för tillsynsmyndighetens verksamhet.

PTS föreslås bli tillsynsmyndighet enligt den nya lagen.

9.6.1 Föreligger det ett behov av ytterligare tillsynsreglering utöver den som gäller i dag?

Den nya lagen om domännamnshantering skall se till att administrationen av den nationella toppdomänen för Sverige utförs i allmänhetens intresse på ett säkert, robust och effektivt sätt. För att säkerställa att de kriterier som lagen eller föreskrifter meddelade med stöd av lagen ställer upp för verksamheten faktiskt efterlevs är det av vikt att en kontrollmöjlighet finns.

I kapitel 6 har utredningen närmare granskat vilka möjligheter som i dag föreligger till statlig tillsyn över administrationen av en nationell toppdomän för Sverige. Av den redovisning som där lämnats framgår att det, utöver vad gäller integritetsskyddet, saknas reella möjligheter att utöva ändamålsenlig statlig tillsyn för att tillse att lagens syfte uppfylls. Varken stiftelselagen eller annan lagstiftning ger möjligheter till ingripanden för att säkerställa att de krav som enligt lag eller annan författning bör ställas upp för driften av toppdomänen, t.ex. för teknisk drift och driftssäkerhet, verkligen uppfylls.

9.6.2 Överväganden

Med hänsyn till dagens avsaknad av möjlighet att kontrollera att administrationen av den nationella toppdomänen för Sverige uppfyller de krav som enligt ovan bör ställas på denna måste en möjlighet att utöva tillsyn införas genom den nya lagen.

Den tillsynsverksamhet som bör bedrivas skall, på sedvanligt sätt, säkerställa att ändamålet med lagen och föreskrifter som har meddelats med stöd av lagen tillgodoses. Tillsynen skall huvudsakligen ske genom s.k. granskande tillsyn i efterhand.

Syftet med tillsynen är att tillsynsmyndigheten skall kontrollera efterlevnaden av lagen och de föreskrifter som har meddelats med stöd av denna. Tillsynen är alltså, med hänsyn till lagens ändamål, huvudsakligen till för att skydda samhällets och medborgarnas intressen av en fungerande och säker Internetanvändning.

För att en effektiv tillsyn skall kunna genomföras måste den ansvariga myndigheten ha möjlighet att bl.a. tillgripa vissa maktmedel i form av sanktioner samt få möjlighet att begära in information eller få tillträde till tillsynsobjektets lokaler, utrustning m.m.

Rätten att begära in information skall endast avse sådan information som behövs i tillsynsverksamheten för vissa angivna ändamål. Huvudsakligen kommer den information som erhålls att ligga till grund för tillsynsverksamheten. Den kan dock även ligga till grund för den utvecklingsuppföljning eller omvärldsanalys som en ansvarig myndighet skall göra inom området för elektronisk kommunikation (jfr SOU 2002:60 och SOU 2002:109).

Om den som är administrativt ansvarig för en nationell toppdomän missköter sin uppgift och inte uppfyller de krav som

ställs på verksamheten i denna lag eller föreskrifter meddelade med stöd av lagen, måste tillsynsmyndighet kunna vidta sanktioner för att åstadkomma rättelse. Tillsynsmyndigheten skall därför ha möjlighet att meddela de förelägganden som behövs för efterlevnaden av lagen eller av nämnda föreskrifter. Ett beslut om föreläggande bör få förenas med vite.

Skulle den administrativt ansvarige trots förelägganden därom ändå inte uppfylla uppställda kriterier för verksamheten och denna misskötsel riskerar Internetanvändningen, kan det finnas skäl att som en tillsynsåtgärd införa ett förbud mot att driva verksamheten vidare. Ett sådant förfarande kräver dock att det finns en ny administrativt ansvarig beredd att ta över verksamheten. En sådan måste dessutom godkännas av ICANN enligt GAC:s principer. Ett förbud i sig skulle därför ha mindre betydelse. Det finns därför inte skäl att införa denna möjlighet till sanktion i lagen. Skulle misskötseln äventyra Internetanvändningen bör istället tillsynsmyndigheten anmäla detta för regeringen som i sin tur kan besluta att ta kontakt med ICANN för att den vägen inleda ett omdelegeringsförfarande.

För att säkerställa att myndighetens beslut om åtgärder m.m. får genomslag skall myndigheten ha rätt att ansöka om och att få verkställighet hos kronofogdemyndigheten av beslut som avser åtgärder för tillsynen. Vid detta förfarande skall bestämmelserna i utsökningsbalken (1981:774) om sådan verkställighet som avses i 16 kap. 10 § den balken gälla.

För den tillsynsverksamhet som tillsynsmyndigheten har att bedriva skall avgift utgå. Den administrativt ansvarige för den nationella toppdomänen för Sverige är som huvudsakligt tillsynsobjekt den som naturligen har att betala denna avgift. Hur avgiften skall beräknas bör regeringen eller den myndighet regeringen bestämmer meddela närmare föreskrifter om.

Inom ramen för den försöksverksamhet som PTS på uppdrag av regeringen har bedrivit för att undersöka om Internet kan fungera oberoende av funktioner utomlands har PTS erhållit stor inblick i hur säkerhet i administrationen av toppdomänen *se* bör kunna utformas. Det har även, enligt uppgifter som utredningen har fått, framförts önskemål från II-stiftelsens sida om samarbete med PTS och sådant har i någon mån etablerats. Det kan därför finnas skäl att PTS blir den myndighet som utövar tillsyn och meddelar föreskrifter enligt lagen. PTS bör även ges mandat att genomföra

prov av Internets robusthet m.m. såvitt avser det av lagen omfattade tillämpningsområdet.

10 Övriga frågor

10.1 Myndighetsutövning

I samband med Domännamnsutredningens arbete framfördes uppfattningen att tilldelningsförfarandet, som då innefattade en förprövning av en ansökan innan registrering beviljades, kunde anses utgöra myndighetsutövning. Det anfördes bl.a. att stora likheter förelåg med Patent- och registreringsverkets (PRV) handläggning av varumärkesansökningar.

Domännamnsutredningen fann att den allmänna uppfattningen var att den då gällande domännamnsadministrationen var myndighetslik, främst till följd av systemet med förprövning och de regler som styrde den. Något egentligt ställningstagande till om hanteringen av toppdomänen *se* innebar myndighetsutövning gjordes dock inte. För att komma till rätta med problemet föreslog utredningen istället att förprövningen, som i stor utsträckning ansågs utgöra kärnproblemet, skulle slopas och regelverket ändras så att alla som ansöker om domännamn som huvudregel skall få registrera dessa. En sådan hantering ansåg Domännamnsutredningen inte innefatta myndighetsutövning.

Sedan Domännamnsutredningens betänkande har förfarandet med förprövning av ansökningar om domännamn avskaffats och reglerna för hur tilldelning skall ske ändrats.

Frågan är emellertid om den reglering av administrationen av den nationella toppdomänen för Sverige som vi nu föreslår medför att myndighetsutövning uppkommer.

Som framgått är det utredningens ståndpunkt att administrationen av toppdomänen *se* alltjämt skall bedrivas i privaträttslig regi genom II-stiftelsens försorg. Enligt 11 kap. 6 § tredje stycket RF får en förvaltningsuppgift överlämnas till bolag, förening, samfällighet, stiftelse, registrerat trossamfund eller någon av dess organisatoriska delar eller till enskild individ. Om förvaltningsuppgiften innefattar myndighetsutövning måste överlämnandet ske med stöd

av lag. Kravet på lagform utgör en garanti för att medborgarnas intressen inte blir åsidosatta. Det bör dock vara tillräckligt att ett medgivande till överlämnandet finns i lag.[1]

Med hänsyn till regleringen i RF finns det skäl att speciellt se närmare på om tilldelningen av domännamn under toppdomänen *se* är att betrakta som en sådan offentlig förvaltningsuppgift som där avses och, om så är fallet, om den innefattar myndighetsutövning. Detta gäller speciellt då utformningen av en reglering kan komma att påverkas därav.

10.1.1 Förvaltningsuppgift och myndighetsutövning?

Enligt 11 kap. 6 § RF finns det offentliga förvaltningsuppgifter av olika karaktär, dels ”ordinära” förvaltningsuppgifter, dels sådana som innefattar myndighetsutövning. I förarbetena till RF anges endast i allmänna ordalag vad som avses med begreppet offentlig förvaltningsuppgift. Departementschefen beskriver begreppet som dels ”verksamhet som innefattar förvaltning för det allmännas räkning”, dels ”förvaltningsuppgift som det allmänna har” (prop. 1973:90 s 396 f). Något egentligt klargörande av vad som skall förstås med begreppet offentlig förvaltningsuppgift innebär uttalandet inte.[2] För att kunna avgöra vad som avses med en offentlig förvaltningsuppgift är det nödvändigt att ta utgångspunkt i begreppet offentlig förvaltning. Sådan förvaltning regleras i 11 kap. RF.

Förenklat kan offentlig förvaltning[3] uttryckas vara den verksamhet som utförs av förvaltningsmyndigheterna. Emellertid utgör regeringen, de beslutande församlingarna (t.ex. riksdagen och kommunernas fullmäktige) och domstolarna inte förvaltningsmyndigheter enligt RF:s begreppsbildning. Dessa, liksom enskilda subjekt med stöd av 11 kap. 6 § tredje stycket RF, kan dock utföra vissa förvaltningsuppgifter. Sådana uppgifter kan gälla handläggningen av enskilda fall enligt gällande lagar och förordningar.

Den verksamhet som enligt RF åvilar riksdag och regering är, i den mån verksamheten inte avser enskilda fall, undantagen från vad som anses utgöra förvaltning. Detta gäller även domstolarnas rättskipande verksamhet. Offentlig förvaltning kan alltså sägas utgöra

[1] Jfr Petrén, Gustaf/Ragnemalm, Hans, Sveriges grundlagar, 12:e uppl., s. 279 och 281 f.
[2] Se bl.a. Petrén/Ragnemalm, a.a., s. 277.
[3] För närmare definition av begreppet offentlig förvaltning se Strömberg, Håkan, Allmän förvaltningsrätt, 21:a uppl., s. 16 ff., samt Ragnemalm, Hans, Överlämnande av förvaltningsuppgift till enskilt subjekt, Förvaltningsrättslig tidsskrift 1976 s. 105 – 145.

vad som återstår av offentlig verksamhet sedan man undantagit vissa andra mer lättdefinierade funktioner, särskilt normgivning, budgetreglering och rättskipning.[4] Kvar av offentlig verksamhet torde då vara vad som kan hänföras till rättslig och faktisk förvaltningsverksamhet. Med rättslig förvaltningsverksamhet förstås meddelandet av rättsliga direktiv för faktisk sådan verksamhet eller för enskildas handlande. Med faktisk förvaltningsverksamhet förstås själva utförandet av en förvaltningsuppgift, t.ex. service och rådgivning, byggande och underhåll av vägar samt tillhandahållande av sjukvård och undervisning m.m.

Också verksamhetens materiella innebörd och ändamål måste emellertid beaktas vid bestämmandet av begreppet offentlig förvaltning. Inom doktrinen har ett antal kriterier ställts upp för att avgöra vad som kännetecknar offentlig förvaltning och en därmed sammanhängande förvaltningsuppgift.

Ett kriterium tar sin grund i att den offentliga förvaltningen tar sin utgångspunkt i ett *offentligt ändamål eller intresse* medan den enskilda verksamheten istället drivs i vinstsyfte.[5] Emellertid finns det sådana avgörande undantag från denna huvudregel att den inte kan användas som en juridisk avgränsning för att fastställa vad som skall anses utgöra offentlig förvaltning. Också offentlig förvaltning kan bedrivas i vinstsyfte och enskild verksamhet kan vara samhällsnyttig på ett sådant sätt att staten måste ta över verksamheten om den missköts eller upphör.

En omständighet som huvudsakligen skiljer den offentliga förvaltningsverksamheten från enskild sådan är att den offentliga förvaltningen tar sitt ursprung i *författningar eller andra beslut* av riksdagen eller regeringen. De ansvarsuppgifter som den offentliga förvaltningen har att uppfylla följer till stor del av offentligrättsliga regleringar och av beslut av regeringen eller riksdagen. Offentligrättsliga regleringar kan ges i form av lagar eller förordningar med instruktioner. Uppgifter kan även ges i t.ex. regleringsbrev. De offentligrättsliga regler som ställs upp för den offentliga förvaltningsverksamheten innebär inte sällan maktbefogenheter genom möjlighet att rikta åligganden eller förbud mot enskilda. Reglerna ställer ofta även upp rättssäkerhetsgarantier i form av t.ex. överklagandemöjligheter.

Den normbundenhet som följer av 1 kap. 1 § RF – som anger att den offentliga makten utövas under lagarna – innebär att den som

[4] Se Strömberg, a.a., s. 16.
[5] Se Strömberg, a.a., s. 18.

utövar en offentlig förvaltningsuppgift måste utföra denna på ett sätt som stämmer överens med gällande lagar och andra författningar och också i övrigt tillgodoser de allmänna medborgarintressena. Det är staten som har ansvaret för att så sker (prop. 1975/76:209 s. 166). Normbundenheten begränsar, till skillnad från vad som gäller för enskild verksamhet, handlingsfriheten vid t.ex. avtals ingående för den som har att utföra en offentlig förvaltningsuppgift. En omständighet som kan skilja den offentliga förvaltningsverksamheten från enskild sådan är alltså att uppgiften grundar sig på en författning eller något annat beslut av regeringen eller riksdagen.

Det anförda leder till slutsatsen att det är svårt, rent av ogörligt, att bestämma vad som avses med offentlig förvaltning utifrån generella kriterier.[6] En bedömning måste ske från fall till fall vid viss tidpunkt. I fråga om viss art av förvaltningsverksamhet är avgränsningen dock tydligare. Det gäller när de offentligrättsliga reglerna ger möjlighet att utöva offentlig makt genom myndighetsutövning.

Det i 11 kap. 6 § tredje stycket RF använda begreppet myndighetsutövning har, enligt uttalanden i förarbetena till RF, samma innebörd som enligt den då gällande äldre förvaltningslagen (1971:290), ÄFL (prop. 1973:90 s. 397). Någon förändring av begreppets innebörd har inte avsetts eller skett genom införandet av den nu gällande förvaltningslagen (1986:223), FL (prop. 1985/86:80 s. 55).

Med myndighetsutövning avses enligt FL utövning av befogenhet att för enskild bestämma om förmån, rättighet, skyldighet, disciplinpåföljd eller annat jämförbart förhållande (prop. 1971:30 s. 330 ff.). Det utmärkande för all myndighetsutövning är att det rör sig om beslut eller andra åtgärder som ytterst är uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Det kan gälla såväl åläggande av förpliktelser m.m. som för den enskilde gynnande beslut.

Den redovisade definitionen av begreppet ger en allmän ram för vad som skall anses utgöra myndighetsutövning. Denna ram måste dock preciseras ytterligare.

För det första måste det föreligga en *befogenhet att utöva myndighetsutövning* och befogenheten skall utövas i förhållande till enskild (prop. 1971:30 s. 331). Befogenheten måste, såsom gäller för

[6] Se bl.a. Strömberg, a.a., s. 18, samt Ragnemalm, a.a., s. 111.

förvaltningsuppgifter, grunda sig på lag eller annan författning eller på annat sätt kunna härledas ur ett bemyndigande av regeringen eller riksdagen (prop. 1971:30 s. 334).

Den för begreppet myndighetsutövning använda definitionen innebär genom orden ”bestämma om” att från myndighetsutövning undantas andra ärenden än sådana där myndigheten *ensidigt genom beslut avgör saken*. Detta innebär dels att endast ärenden som mynnar ut i bindande beslut omfattas av begreppet myndighetsutövning, dels att ärenden som avgörs genom att myndigheterna träffar avtal eller överenskommelse med någon enskild undantas från samma begrepp. Myndigheten har alltså att ensidigt pröva om de i författning givna förutsättningarna för att förplikta den enskilde något föreligger eller om den enskilde uppfyller de angivna förutsättningarna för att få en förmån eller en rättighet, t.ex. tillstånd att bedriva en viss verksamhet.[7]

Det klargörs i förarbetena till ÄFL att med bindande beslut avses inte endast sådana slutliga beslut som avgör ärendet i sak. Även beslut genom vilka myndigheterna skiljer ärendet ifrån sig utan sakprövning, t.ex. avskrivnings- och avvisningsbeslut, faller in under begreppet myndighetsutövning.

I förarbetena till ÄFL uttalas vidare att karakteristiskt för myndighetsutövning är att den enskilde befinner sig i ett slags *beroendeförhållande* (prop. 1971:30 s. 331) gentemot det allmänna. Är det fråga om ett beslut genom vilket den enskilde förpliktas att göra, tåla eller underlåta något – t.ex. ett förbud, ett föreläggande eller liknande – måste denne rätta sig efter beslutet, eftersom tvångsmedel av något slag annars kan användas mot den enskilde. Om det istället rör sig om ett gynnande beslut kommer beroendeförhållandet istället till uttryck genom att den enskilde är tvingad att vända sig till en myndighet för att få en förmån eller en rättighet och att myndighetens tillämpning av de på området gällande författningsbestämmelserna blir av avgörande betydelse för honom. Det är alltså det allmänna som ensamt har möjlighet att tillmötesgå den enskildes anspråk och därigenom utöva makt mot denne.

Begreppet myndighetsutövning innefattar även ärenden som avser meddelande av föreskrift till allmän efterrättelse, s.k. normbeslut (prop. 1971:30 s. 335). Till myndighetsutövning bör vidare hänföras sådana beslut som i och för sig inte innehåller handlingsdirektiv för den enskilde men som medför indirekta rätts-

[7] Se bl.a. Petrén/Ragnemalm, a.a., s. 279.

verkningar gentemot denne genom att beslutet är avsett att ligga till grund för meddelande av betungande eller gynnande handlingsmönster.[8] Sådana kan utgöras av t.ex. registreringsbeslut och beslut om utfärdande av legitimationshandlingar.[9] Att registreringsbeslut, som till synes inte medför annat än en anteckning om ett visst förhållande, kan utgöra myndighetsutövning beror på att registreringen kan medföra indirekta rättsverkningar. En registrering kan t.ex. tjäna som rättsfaktum enligt skilda rättsregler. Så är fallet vad gäller folkbokföringsregister där anteckningen om hemvist fungerar som ett kvalificeringsbeslut med rättsverkningar för t.ex. skattskyldighet och inskrivning hos allmän försäkringskassa.[10]

Det anförda visar på att begreppet myndighetsutövning är tämligen komplext och i viss mån svårt att avgränsa och tillämpa. Som utgångspunkt kan sägas att vissa kumulativa kriterier skall vara uppfyllda för att det skall vara fråga om myndighetsutövning i RF:s mening.

- Det skall föreligga en på författning eller annat bemyndigande från regering eller riksdag grundad befogenhet att utöva myndighetsutövning mot en enskild.
- Den ansvariga myndigheten skall ensidigt genom beslut avgöra saken.
- Den enskilde skall befinna sig i ett slags beroendeförhållande till den aktuella myndighetsutövaren.

10.1.2 Innefattar administrationen av toppdomänen *se* myndighetsutövning?

II-stiftelsen administrerar idag den nationella toppdomänen för Sverige. Uppdraget har II-stiftelsen fått delegerat till sig av IANA, som nu uppgått som en del av ICANN. Delegationen har tillkommit utan inblandning av den svenska staten. Den faktiska driften av toppdomänen utförs enligt ett licensavtal av II-stiftelsens dotterbolag NIC-SE på uppdrag av stiftelsen.

Administrationen av toppdomänen *se* innefattar ett antal olika moment, bl.a. att driva relevanta databaser, den s.k. who is-tjänsten och namnservrar för toppdomänen, att registrera domännamn samt

[8] Se Petrén/Ragnemalm, a.a., s. 280.
[9] Strömberg, a.a., s. 20.
[10] Strömberg, a.a., s. 60.

att tillgängliggöra och distribuera zonfiler för toppdomänen. Av uppgifterna är det speciellt tilldelningen av domännamn efter ansökan och den därmed sammanhängande registerföringen över de tilldelade domännamnen som är av intresse i nu aktuellt sammanhang.

Vid tilldelning och registrering av domännamn under *se* måste man gå vägen via ett av NIC-SE:s många ombud. Ombudet tillhandahåller ansökningsblanketter, allmänna villkor samt information om de kostnader som är förenade med en registrering. Ansökan sänds därefter till NIC-SE, som behandlar ansökningarna i den turordning de kommer in. Hos NIC-SE bedöms ansökan i enlighet med de privaträttsligt upprättade regler som finns för registrering av domäner under *se*. När ansökan är behandlad, meddelar NIC-SE ombudet om ansökan blivit godkänd eller ej. Ombudet meddelar resultatet till den som ansökt om domännamnet.

Det saknas idag offentligrättslig reglering eller annat beslut från den svenska staten som berör administrationen av den nationella toppdomänen för Sverige och bemyndigar II-stiftelsen att utöva detta uppdrag. Det regelsystem som gäller för tilldelning av domännamn under *se* utgörs av s.k. självreglering. Reglerna har antagits av II-stiftelsen efter samarbete med den till stiftelsen knutna privaträttsliga nämnden för domännamnsregler (NDR). Som framgått ovan föreslår vi inte någon ändring i denna del.

Uppgiften att administrera den nationella toppdomänen för Sverige företer ett antal drag som i sig talar för att den skall anses utgöra en offentlig förvaltningsuppgift. I bl.a. kapitel 4 konstaterade vi att den nationella toppdomänen för Sverige utgör en allmänhetens resurs för vilken staten har det övergripande ansvaret. Denna uppfattning återfinns i de grundläggande dokument som gäller för verksamheten, speciellt RFC 1591 och GAC:s principer, uttryckt så att uppgiften att administrera toppdomänen skall ses som ett förtroendeuppdrag och tillhandahållande av samhällsservice i allmänhetens intresse på begäran av såväl den lokala gemenskapen som den globala Internetgemenskapen.

Även det klara ställningstagandet i GAC:s principer för att respektive stat skall ha den övergripande kontrollen och ansvaret för hur den egna nationella toppdomänen administreras talar för att administrationsuppgiften bör anses som ett offentligt intresse och, som sådant, en statsangelägenhet. GAC har dessutom antagit den allmänna principen att Internets namnsystem är en offentlig nyttig-

het i den meningen att dess funktioner måste administreras i allmännyttans intresse. Det anges även i artikel 9.3 i GAC:s principer att det vid underkontraktering av den tekniska hanteringen av toppdomänregistret eller av dess administrativa funktioner m.m. måste klargöras att själva uppdraget är att betrakta som offentlig maktutövning.

Det krävs i princip författningsstöd eller annat beslut av regeringen eller riksdagen för att en offentlig förvaltningsuppgift skall uppkomma. I avsaknad av offentligrättslig reglering eller annat återknytande till statsorganen kan de till administrationen av toppdomänen *se* knutna uppgifterna – t.ex. att tilldela sökande domännamn eller att föra ett register över tilldelade domännamn med kontaktinformation – inte sägas utgöra offentliga förvaltningsuppgifter. Uppgifterna kan då än mindre anses utgöra myndighetsutövning.

Den lag vi nu föreslår skall gälla för administrationen av den nationella toppdomänen för Sverige anger de huvudsakliga kriterier som skall vara uppfyllda i verksamheten. Lagen innehåller inte någon regel som bemyndigar den administrativt ansvarige att utöva uppdraget att administrera nämnda toppdomän. Den anger bara vad denne skall uppfylla vid utövandet av verksamheten. Uppdraget att administrera den nationella toppdomänen i Sverige kommer därför alltjämt att utföras med stöd av den befogenhet som kan härledas ur avtalet med IANA, numera ICANN. Och skulle den som är administrativt ansvarig missköta sitt uppdrag kan staten inte ensidigt bestämma att annan skall utföra uppdraget. En sådan åtgärd förutsätter att ICANN och DoC beslutar att dirigera om den s.k. rotservern. Den reella beslutsmakten över vem som skall ansvara för administrationen får därför närmast sägas tillkomma de båda sistnämnda organen.

Mot denna bakgrund är det utredningens uppfattning att administrationen av den nationella toppdomänen för Sverige inte, trots det bakomliggande offentliga intresset, utgör en offentlig förvaltningsuppgift. Administrationen kan följaktligen därmed inte heller anses utgöra myndighetsutövning.

10.2 Ersättningsfrågor

Av vårt lagförslag framgår att den som har det administrativa ansvaret för den nationella toppdomänen för Sverige är skyldig att tillhandahålla tillsynsmyndigheten en säkerhetskopia av det register som innehåller uppgifter om beviljade domännamn. Dessutom åläggs den administrativt ansvarige en skyldighet att överföra de registerdata som finns i databasen till en ny ansvarig för toppdomänen *se* om administrationen upphör. Som framhållits tidigare i kapitel 7 kan det uppkomma immaterialrättsliga rättigheter till databasen för den som administrerar toppdomänen för Sverige. De rättigheter som det kan vara fråga om är knutna till databasen och den sammanställning av uppgifter som finns i databasen. Mot denna bakgrund måste det diskuteras hur lagförslagets bestämmelser förhåller sig till de grundlagsfästa reglerna om skydd för egendom som återfinns i 2 kap. 18 § RF och om det krävs att det införs någon bestämmelse i lagförslaget som reglerar i vilka fall och i vilken omfattning den som innehar de immaterialrättsliga rättigheterna har rätt till ersättning för intrång i dessa rättigheter.

10.2.1 Något om egendomsskyddet i 2 kap. 18 § RF

I 2 kap. 18 § första stycket RF stadgas att varje medborgares egendom är tryggad genom att ingen kan tvingas avstå sin egendom till det allmänna eller till någon enskild genom expropriation eller något annat sådant förfogande eller tåla att det allmänna inskränker användningen av mark eller byggnad utom när det krävs för att tillgodose angelägna allmänna intressen.

Bestämmelsen i 18 § är inte begränsad till att avse någon viss typ av egendom, utan omfattar både lös och fast egendom. Också särskild rätt till egendom med ekonomiskt värde såsom nyttjanderätt och immaterialrättsliga rättigheter omfattas av bestämmelsen.[11] Det skydd som följer av bestämmelsen gäller för såväl fysiska som juridiska personer.[12] Genom regleringen i 2 kap. 22 § första stycket nionde punkten RF likställs utlänning med svensk medborgare.

Egendomsskyddet i 2 kap. 18 § första ledet RF är begränsat till expropriation eller annat sådant förfarande som sker med stöd av expropriationslagen (1972:719) eller annan lagstiftning. I förarbete-

[11] Se bl.a. Petrén/Ragnemalm, a.a., s. 85 och Nergelius, J, Konstitutionellt rättighetsskydd, Svensk rätt i ett komperativt perspektiv, s. 558 f.
[12] Se prop. 1993/94:117 s. 48.

na sägs att bestämmelsen tar sikte på olika typer av tvångsövertaganden av förmögenhetsrätt som innebär ett överförande eller ianspråktagande av en sådan rätt.[13] Det egendomsskydd som medborgarna garanteras i 2 kap. 18 § RF är emellertid inte absolut. Ett expropriativt ingrepp kan nämligen vara tillåtet om det motiveras av ett angeläget allmänt intresse.[14] Vad som kan anses utgöra ett intresse som motiverar ett ingrepp måste avgöras efter en bedömning i det enskilda fallet. Hänsyn kan därvid tas till politiska värderingar. Särskilt måste beaktas vad som är godtagbart från rättssäkerhetssynpunkt i ett modernt och demokratiskt samhälle.

I förarbetena anges som tillåtna ingrepp i första hand sådana som motiveras av intresset att kunna tillgodose allmänhetens berättigade krav på en god miljö och möjligheterna att kunna bevara och skydda områden som är av särskild betydelse från naturvårdssynpunkt, liksom intresset av att kunna ge allmänheten tillgång till naturen för rekreation och friluftsliv. Utöver de här nämnda miljöaspekterna måste också samhällets behov av mark för anläggande av vägar och andra kommunikationsleder kunna tillgodoses.

Den som tvingas att avstå sin egendom genom expropriation eller annat sådant förfogande är berättigad till ersättning för förlusten enligt 2 kap. 18 § andra stycket RF. Ersättningen skall bestämmas enligt grunder som anges i lag. Den ersättning som skall utgå får därvid inte bara vara symbolisk.[15]

10.2.2 Något om Europakonventionens äganderättsskydd

I förarbetena till bestämmelsen i 2 kap. 18 § RF sägs att innebörden av begreppet ”angeläget allmänt intresse” anknyter till vad som gäller egendomsskyddet i den europeiska konventionen angående skydd för de mänskliga rättigheterna och friheterna.[16]

Enligt artikel 1 i första tilläggsprotokollet till konventionen har varje fysisk eller juridisk person rätt till respekt för sin egendom. Ingen får berövas sin egendom annat än i det allmännas intresse och under de förutsättningar som anges i lag och i folkrättens allmänna grundsatser. Det klargörs dock att bestämmelsen inte

[13] Se prop. 1993/94:117 s. 49.
[14] A.a., s. 48 f.
[15] Se Petrén/Ragnemalm, a.a., s. 85.
[16] Konventionen gäller som svensk rätt genom lagen (1994:1219) om de europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, som trädde i kraft den 1 januari 1995.

inskränker en stats rätt att genomföra sådan lagstiftning som staten finner nödvändig för att bl.a. reglera nyttjandet av egendom i överensstämmelse med det allmännas intresse.

Egendomsbegreppet i artikeln har getts en autonom och vidsträckt innebörd. Begreppet omfattar därför inte enbart äganderätt till fast och lös egendom i civilrättslig mening. Även fordringar och immateriella rättigheter skyddas av artikeln.[17] Utöver vad nu nämnts omfattas legitima förväntningar om ekonomiska förmåner som bygger på existerande rättigheter samt ekonomiska intressen och förväntningar som har samband med utövandet av näringsverksamhet av skyddet.[18]

Enligt Europadomstolens praxis innehåller den ifrågavarande artikeln tre regler.[19] Den första fastslår principen om att egendom skall respekteras. Den andra uppställer villkoren för berövande av egendom. Slutligen behandlar den tredje hur ägarens rätt att utnyttja sin egendom får begränsas.

För att någon skall få berövas äganderätten till sin egendom krävs det att åtgärden vidtas i det allmännas intresse, att det sker i enlighet med förutsättningar som anges i lag och att folkrättens allmänna grundsatser iakttas. I första hand är det de nationella organen som skall göra bedömningen av vad som utgör det allmännas intresse och de har därvid tillerkänts en betydande bedömningsfrihet, s.k. margin of appreciation.[20] Europadomstolen kan emellertid överpröva om denna frihet har utövats på ett rimligt och proportionerligt sätt och om de nationella organens bedömning av vad som är i det allmännas intresse uppenbarligen saknar rimlig grund.[21]

Även om det i och för sig föreligger ett allmänt intresse som kan motivera ett berövande av egendom innebär det uppställda kravet på proportionalitet att domstolen vid sin prövning gör en avvägning mellan det allmännas intresse och det men som den enskilde lider. För att äganderätten skall få kränkas måste det

[17] Se t.ex. Danelius, H, Mänskliga rättigheter i europeisk praxis, En kommentar till Europakonventionen om de mänskliga rättigheterna, 2002, s. 374.
[18] Se t.ex. Van Marle m.fl. mot Nederländerna, dom 1986-06-26, Ser. A Vol. 101; Tre Traktörer Aktiebolag mot Sverige, dom 1989-07-07, Ser. A Vol. 159; Fredin mot Sverige, dom 1991-02-18, Ser. A Vol. 192 samt RÅ 2001 ref 72.
[19] Se Danelius, a.a., s. 375 f.
[20] Se Nergelius a.a., s. 534 f.
[21] Se Danelius, a.a., s. 376 samt även bl.a. James m.fl. mot Storbritannien, dom 1986-02-21, Ser. A Vol. 98-B och Pressos Compania Naviera S.A. m.fl. mot Belgien, dom 1995-11-20, Ser. A Vol. 332.

föreligga en skälig balans mellan de olika intressena. Ingreppet får inte innebära att den enskilde åläggs en oproportionerlig börda.

Vid bedömningen av om ingreppet är proportionerligt är det av stor betydelse om den enskilde tillerkänns ersättning i någon form. Det krävs emellertid inte att full ersättning skall lämnas under alla förhållanden.

Krav på att ett egendomsberövande endast får ske ”under de förutsättningar som anges i lag” innebär inte bara att det skall finnas stöd för åtgärden i nationell lag.[22] Det ställs också krav på att den nationella lagen skall vara tillgänglig och tillräckligt precis för att göra ingreppet i äganderätten förutsebart samt att lagens innehåll tillgodoser rimliga rättssäkerhetskrav.

Med expropriation som har lagligt stöd kan likställas ett ingrepp som inte formellt betecknas som expropriation men som är av sådant slag att ägaren i realiteten berövas alla sina rättigheter som ägare, s.k. expropriation de facto. Ett sådant de facto berövande anses föreligga när stora ingrepp sker i den enskildes äganderätt utan att det juridiska ägandet till egendomen förändras. Prövningen av om ett aktuellt ingrepp är vid handen skall i första hand ta avstamp i om ingreppet i praktiken får samma konsekvenser som ett formellt egendomsberövande, snarare än utifrån de ekonomiska konsekvenserna.[23] Europadomstolen har dock visat stor restriktivitet med att konstatera berövanden av detta slag.

Bestämmelsen om att varje fysisk eller juridisk person har rätt till respekt för sin egendom har enligt Europadomstolens praxis en självständig betydelse utöver vad som i övrigt föreskrivs i artikeln. Trots att det varken är fråga om ett egendomsberövande eller en inskränkning i rätten att utnyttja egendom, kan ett ingrepp i äganderätten under vissa omständigheter alltså ändå anses föreligga.[24]

10.2.3 Överväganden

Vårt förslag: Lagförslaget bör innehålla en bestämmelse som ger den som är skyldig att överföra registerdata i samband med att administrationen av den nationella toppdomänen för Sverige upphör rätt till skälig ersättning.

[22] Se Danelius, a.a., s. 383.
[23] Se Ullenhag, Erik, SvJT 1998, Kärnkraftsavvecklingen och Europakonventionen, s. 322 med vidare hänvisning i noterna 38–40 samt 42–44.
[24] Se Danelius, a. a., s. 391.

Som vi konstaterat i kapitel 7 kan det föreligga ett upphovsrättsligt skydd för den databas som ingår i administrationen av toppdomänen *se*. I vart fall föreligger med största sannolikhet ett upphovsrättsligt katalogskydd för de uppgifter som sammanställts i databasen. Båda dessa typer av rättigheter omfattas av 2 kap. 18 § RF och är alltså skyddade gentemot de ingrepp, dvs. expropriation eller annat liknande förfogande, som avses i bestämmelsen.

Vårt lagförslag omfattar två situationer där man bör diskutera om de skyldigheter som följer av lagen innebär intrång i rättigheter som kan tillkomma den som ansvarar för den nationella toppdomänen. Den första situationen är den som innebär en skyldighet för den administrativt ansvarige för toppdomänen att tillhandahålla en kopia av registret över beviljade domännamn till tillsynsmyndigheten. Den andra rör skyldigheten att överföra registerdata till tillsynsmyndigheten eller en ny administrativt ansvarig i samband med att administrationen upphör.

Vad gäller den första situationen syftar skyldigheten för den som har det administrativa ansvaret för toppdomänen till att säkerställa att det finns en säkerhetskopia. Det är i det sammanhanget inte meningen att tillsynsmyndigheten eller annan skall förfoga över kopian på ett sätt som utgör ett intrång i äganderätten eller någon annan rätt. Med stöd av denna bestämmelse i lagförslaget kommer alltså varken tillsynsmyndigheten eller annan att kunna ändra, vidarebefordra, framställa egna kopior av säkerhetskopian eller på annat sätt förmögenhetsrättsligt avhända innehavaren den immateriella rättigheten.

I lagförarbetena till RF har, som redovisats ovan, uttalas att man med uttrycket expropriation eller annat sådant förfogande avser olika former av tvångsövertaganden av förmögenhetsrätt som innebär ett överförande eller ianspråktagande av egendom. Också i doktrinen har man framhållit att expropriation eller annat sådant förfarande som talas om i 2 kap. 18 § RF måste innebära just ett avstående av äganderätt eller motsvarande rätt med ekonomiskt värde, såsom nyttjanderätt eller servitut.[25] Skyldigheten för en administrativt ansvarig att tillhandahålla en säkerhetskopia utan att tillsynsmyndigheten ges rätt att förfoga över denna på annat sätt än att förvara kopian kan mot bakgrund av uttalandena knappast utgöra ett sådant ianspråktagande av en egendomsrätt som 2 kap. 18 § RF avser.

[25] Se Petrén/Ragnemalm, a.a., s. 85.

Vad däremot gäller den andra situationen är syftet att de registerdata som finns i den administrativt ansvariges databas skall föras över för att tillsynsmyndigheten eller en ny administrativt ansvarig skall förfoga över dem på samma sätt och i samma utsträckning som den ursprunglige administratören. I ett sådant fall får det anses klart att förpliktelsen för den som har det administrativa ansvaret för toppdomänen att överlämna registerdata innebär ett tvångsövertagande av den sammanställning som omfattas av upphovsrätt eller i vart fall katalogskydd. Av intresse är därmed om ingreppet i katalogskyddet kan sägas tjäna ett så angeläget allmänt intresse att tvångsövertagandet trots bestämmelsen i 2 kap. 18 § RF är tillåtet.

Förpliktelsen att överföra databasen kommer att aktualiseras i ett mycket begränsat antal fall där det står klart att ansvaret för administrationen måste flyttas över till annan ansvarig. Så kan exempelvis vara fallet om den som har det administrativa ansvaret försatts i konkurs eller vid upprepade tillfällen misskött uppdraget på ett sådant sätt att en överflyttning av administrationen har ansetts nödvändig för att toppdomänen skall fungera. De allmänna intressena av att kunna garantera en robust, säker och fungerande nationell toppdomän kommer i dessa fall att vara påtagliga. I sammanhanget bör också framhållas att rätten att besluta att administrationen av toppdomänen skall överföras på annan i realiteten vilar på ICANN och DoC som förfogar över de s.k. rotservrarna.

Den som har det administrativa ansvaret för en nationell toppdomän har inte någon äganderätt eller annan rätt till toppdomänen som gör att administrationen kan överlåtas till annan på ett sätt som kan vara fallet med andra rörelser. Däremot kan den som har det administrativa ansvaret för toppdomänen överlåta ett register som upprättas i och med utövandet av administrationen. Oavsett om den administrativt ansvarige kommer att ha kvar en rättighet till den sammanställning av uppgifter som finns i en databas kommer sammanställningen emellertid inte längre att kunna användas för det syfte som den ursprungligen upprättats. Detta leder till att rättighetens värde i samband med ett överflyttande får anses betydligt reducerat. Det innebär emellertid inte att registret inte kan överlåtas för att användas för ett annat syfte och att det i ett sådant sammanhang kan betinga ett visst värde.

Det allmänna intresset av att den nationella toppdomänen för Sverige fungerar på ett sätt som tillgodoser allmänna intressen

måste av det ovan anförda anses stå i proportion till följden av ingreppet i den immaterialrättsliga rättigheten. Detta särskilt om innehavaren av rättigheten har rätt till viss ersättning. En sådan ersättningsbestämmelse bör anknyta till URL och medge ersättning för det intrång i upphovsrätten till katalogskyddet som överlämnandet av en säkerhetskopia och ett övertagande av administrationen av den nationella toppdomänen för Sverige kan komma att innebära.

Sammanfattningsvis kan vi alltså konstatera att lagförslaget bör innehålla en reglering som ger rätt till skälig ersättning för att registerdata flyttas över i samband med att administrationen av den nationella toppdomänen övergår på annan.

10.3 Skydd för näringsfriheten

I och med genomförandet av det lagförslag som vi presenterar kommer den som har det administrativa ansvaret för den nationella toppdomänen att åläggas vissa ekonomiska förpliktelser. Detta bl.a. genom den i lagen föreskrivna skyldigheten att tillse att de avgifter som utgår i samband med namntilldelningen skall vara skäliga. Därtill kommer att den som har det administrativa ansvaret åläggs att betala tillsynsavgift till staten. Fråga uppkommer därmed om förpliktelserna innebär sådana begränsningar i näringsfriheten som är otillåtna enligt 2 kap. 20 § RF.

Bestämmelsen i 2 kap. 20 § RF tar sikte på den s.k. likhetsprincipen. Denna princip kan kortfattat sägas innebära att alla regleringar på närings- och yrkesfrihetens område måste vara generella på så sätt att alla skall ha möjlighet att konkurrera på lika villkor under förutsättning att de i övrigt uppfyller de krav som kan ställas upp för just det yrket eller den näringsgrenen.

I det första ledet i 2 kap. 20 § RF sägs att begränsningar i rätten att driva näring får införas bara för att skydda allmänna intressen. Med sådant intresse avses enligt förarbeten att syftet med inskränkningen är att skydda något som ur samhällets synpunkt anses skyddsvärt. Vad som närmare skall anses ingå i begreppet och hur en bedömning skall ske utvecklas inte närmare i förarbetena till bestämmelsen.[26] I stället hänvisas till vad som anses utgöra ett angeläget allmänt intresse i bestämmelsen om egendomsskyddet i 2 kap. 18 § RF (se avsnitten 10.2.1 och 10.2.2). I likhet med vad

[26] Se prop. 1993/94:117 s. 19 f.

som anförts där måste det slutliga ställningstagandet till vad som är ett sådant intresse som medger undantag från 2 kap. 20 § RF göras från fall till fall i enlighet med vad som kan anses acceptabelt i ett demokratiskt samhälle.[27]

Syftet med den föreslagna lagstiftningen om den nationella toppdomänen *se* är att tillgodose statens behov av att säkra toppdomänen som den kritiska resurs som domänen kommit att utvecklas till. Som vi redovisat i det föregående avsnittet om egendomsskyddet i 2 kap. 18 § RF anser vi att de bakomliggande motiven till lagförslaget utgör ett sådant allmänt intresse som talas om i den bestämmelsen. Eftersom begreppet angelägna allmänna intressen har samma innebörd i 2 kap. 18 och 20 §§ RF bör de bakomliggande motiven till lagen också kunna anses utgöra sådana omständigheter som innebär att den föreslagna lagen inte står i strid med det sistnämnda stadgandet. Här bör också tilläggas att de ekonomiska förpliktelser som följer av lagen inte kommer att innebära något större ingrepp i rätten för den som har det administrativa ansvaret för toppdomänen att driva näring. Den bestämmelse som innebär en begränsning i rätten att bestämma storleken på avgifterna i samband med namntilldelningen lämnar dessutom utrymme för den administrativt ansvarige att påverka avgifternas storlek.

[27] Se prop. 1993/94:117 s. 20 f. och s. 50 f.

11 Behovet av vidare överväganden

Vi har i kapitel 4 framhållit att Internets snabba utveckling mot ökad tillgänglighet och ökad samhällelig betydelse inneburit att ett flertal viktiga frågor ännu inte setts över i samma utsträckning som liknande frågor inom andra närliggande områden. Vårt förslag till en reglering av administrationen av den nationella toppdomänen *se* innebär att vi har analyserat en av de frågor som är av betydelse. Enligt vår mening finns det emellertid också en rad andra viktiga frågor som bör ses över framdeles. Här kan nämnas viktiga frågor för infrastrukturen, såsom knutpunkter, där man enligt vår mening bör föra en diskussion kring statens framtida roll. Detta inte minst för att skapa en överblick över vad det kan finnas ett behov av att garantera för samhällsviktiga funktioner, men också för att kunna göra klart inom vilka områden som det inte behövs någon lagreglering eller annan statlig inblandning.

Om man tar som utgångspunkt att viss del av Internetanvändningen har kommit att bli en samhällsviktig företeelse bör också Internetanvändning göras tillgänglig för så många som möjligt. För att så skall vara fallet krävs emellertid bl.a. att enskilda ges ökade möjligheter till utbildning. Ytterligare en fråga som är av intresse är därmed vilket ansvar staten bör anses ha för att Internetanvändningen skall kunna göras än mer tillgänglig än vad som idag är fallet.

Hur den tekniska utvecklingen inom Internetområdet eller utvecklingen av olika adresseringssystem kommer att se ut framdeles är inte möjligt att uttala sig om inom ramen för vårt uppdrag. Det bör emellertid nämnas att utvecklingen inom olika områden kan leda till att man istället för DNS använder sig av andra lösningar, vilket kan leda till att betydelsen av DNS minskar. Hur man i en sådan situation garanterar det statliga inflytandet över och insynen i viss del av Internetanvändningen bör enligt vår mening utredas vidare. I ett sådant sammanhang bör det också närmare

belysas vilka konsekvenser den ökade Internetanvändningen vad exempelvis gäller betalningstjänster och övervakning av annan infrastruktur får.

12 Konsekvenser av våra förslag

Det lagförslag vi lägger fram i detta betänkande medför vissa finansiella konsekvenser. I detta kapitel redovisar vi vår bedömning av hur lagförslaget påverkar dels kostnaderna för staten, dels små företags villkor. Synpunkter har inhämtats från Näringslivets nämnd för regelgranskning.

12.1 Kostnader för staten

De konsekvenser ur ett ekonomiskt perspektiv som den föreslagna lagen får för staten utgörs huvudsakligen av den nya tillsynsverksamheten. Tillsynsuppgiften bör enligt vårt förslag utföras av sektorsmyndigheten på området för elektronisk kommunikation, dvs. av PTS. Utöver den rena tillsynsverksamheten får tillsynsmyndigheten även i uppgift att följa utvecklingen av Internetanvändningen i stort samt att meddela de närmare föreskrifter som regeringen bemyndigar tillsynsmyndigheten till att utfärda.

Enligt de uppgifter som utredningen erhållit från PTS kommer tillsynsverksamheten uppskattningsvis att kräva ett par årsarbetskrafter. Vid denna bedömning har hänsyn tagits till att, som utredningen föreslagit, tillsynsansvaret även kommer att omfatta viss omvärldsbevakning, provverksamhet etc. Kostnaderna för tillsynsverksamheten enligt lagen om nationell toppdomän kan beräknas uppgå till ett par miljoner kronor.

Utöver den rena tillsynsverksamheten ankommer det på en tillsynsmyndighet att meddela de föreskrifter som behövs i enlighet med eventuellt förordnande av regeringen. Sådana föreskrifter kan avse driftssäkerhet, registerverksamhet m.m. Med hänsyn till att dokumentationen av vad som faktiskt skall uppfyllas i verksamheten knappast kan anses speciellt precis eller klargörande, kan det initialt finnas behov av en punktinsats på föreskriftsområdet. Föreskriftsverksamheten kommer dock att ske mot bakgrund av de

erfarenheter som erhålls vid tillsynsarbetet och torde inte innebära en särskilt betungande uppgift på längre sikt.

Sammanfattningsvis kan konstateras att den statliga tillsyn som vår föreslagna lag om nationell toppdomän föranleder kommer att medföra kostnader för staten. Dessa skall finansieras genom uttag av tillsynsavgift från den som administrerar toppdomänen. Vad i övrigt gäller försöksverksamheter eller andra verksamheter för att skapa säkra elektroniska kommunikationer finansieras dessa idag till delar genom anslag. I den mån sådan verksamhet avser det område som den föreslagna lagen reglerar, bör denna på liknande sätt finansieras genom anslag från statsbudgeten. Någon speciell grund att anta att just administrationen av den nationella toppdomänen skulle generera kostnader nämnvärt utöver vad som följer av PTS nuvarande verksamhet inom området IT-tillit eller IT-tillgänglighet föreligger inte. Någon ändring av finansieringen av sådan verksamhet föreslås alltså inte. Statens merkostnader i anledning av vårt förslag bör alltså sammanfattningsvis kunna finansieras genom tillsynsavgifterna.

12.2 Små företags villkor

När det gäller frågan om eventuell påverkan på små företags villkor genom t.ex. ökade kostnader med anledning av de nya bestämmelserna för den nationella toppdomänen, kan sammanfattningsvis konstateras att företagens kostnader sannolikt kan komma att bli något lägre.

Genom den nya lagen om nationell toppdomän införs statlig tillsyn över den nationella toppdomänen för Sverige. Tillsynsverksamheten skall enligt vårt förslag finansieras via en tillsynsavgift. Vi föreslår att denna avgift skall tas ut från den som administrerar den nationella toppdomänen. Avgiften utgör, enligt vad vi föreskriver, en sådan kostnad som får ligga till grund för den årsavgift som varje domännamnsinnehavare har att betala för domännamnet. Det är därför troligt att den tillsynskostnad om några miljoner kr som kommer att tas ut för PTS verksamhet kommer att övervältras på domännamnsinnehavarna. Med hänsyn till tillsynskostnadens storlek och det antal domännamn som finns registrerade idag, torde tillsynskostnaderna kunna medföra en upp-

skattad höjning av årsavgiften i storleksordningen cirka 10 – 20 kr för varje domännamn.[1]

I den nya lagen finns en regel som innebär att årsavgiften för ett domännamn skall vara skälig. Detta innebär en förändring i förhållande till vad som gäller idag. Av de uppgifter utredningen fått från II-stiftelsen under utredningsarbetet framgår att det inom speciellt NIC-SE:s verksamhet finns ett överskott. Överskott i II-stiftelsens verksamhet skall enligt II-stiftelsen användas i verksamheten eller fonderas för att senare kunna stödja forskning och utbildning inom Internets infrastruktur, allt i enlighet med stiftelsens ändamål. Den ökade registreringen av domännamn ger ökade intäkter för årsavgifter. Under den gångna våren har antalet registrerade domännamn ökat med drygt femtio procent. De intäkter som därigenom inflyter i verksamheten torde knappast motsvaras av utgifter för den faktiska verksamheten till följd av ökningen.

De nya krav som kommer att ställas på administrationen av den nationella toppdomänen kommer med största sannolikhet att innebära vissa kostnadsökningar i verksamheten för utrustning, driftavtal m.m. En del av den intäktsökning som följer av det ökade antalet registrerade domännamn kommer därmed att motsvaras av kostnadsökningar för att uppfylla den nya regleringens krav. Även om det i nuläget är svårt att närmare uppskatta dessa kostnadsökningar är det vår uppfattning att årsavgiften, även med beaktande av de eventuellt ökade kostnaderna till följd av ökningen av antalet registrerade domännamn, snarare kommer att kunna sänkas än höjas med anledning av regeln om ersättningens skälighet.

[1] Enligt uppgift på http://www.nic.se/ uppgick antalet registrerade domännamn till 168 876 stycken den 2003-06-06. Vid årsskiftet uppgick denna siffra till cirka 103 000 st.

13 Författningskommentar

Förslaget till lag om nationell toppdomän för Sverige

Lagens syfte

1 §

Bestämmelserna i denna lag syftar till att säkerställa att administrationen av en nationell toppdomän utförs på ett robust, säkert och effektivt sätt i allmänhetens intresse.

Målsättningsstadgandet i paragrafen gäller samtliga de delar av administrationen av den nationella toppdomänen för Sverige som omfattas av lagen. Det innebär att den tekniska driften samt namntilldelningen och registreringen av domännamn i alla delar skall utföras på ett robust, säkert och effektivt sätt i allmänhetens intresse.

Med robusthet avses bl.a. kapacitet att motstå driftstörningar till följd av fysiska och logiska hot samt personell kompetens hos driftsorganisationerna. Att administrationen skall utföras på ett säkert sätt innebär, förutom att den skall var driftsäker, också att den skall tillgodose bl.a. ett gott integritetsskydd. Effektiviteten i administrationen avser huvudsakligen faktorer som tillgänglighet, dvs. möjligheten att utnyttja en resurs, såsom t.ex. DNS-tjänsten, efter behov i förväntad utsträckning och inom önskad tid, samt användarvänlighet.

Definitioner

2 §

I denna lag avses med

domännamn: beteckning för adressering i ett internationellt domännamnssystem för elektronisk kommunikation,

nationell toppdomän: domän som betecknar Sverige på den högsta nivån i ett internationellt domännamnssystem,

administratör: den som ansvarar för teknisk drift av en toppdomän samt tilldelning och registrering av domännamn,

namnserver: dator i ett elektroniskt kommunikationsnät som programmerats så att den lagrar och distribuerar filer med information om domännamn samt tar emot och svarar på frågor om domännamn i nätet.

Bestämmelsen innehåller definitioner. Bland annat definieras vad som avses med en nationell toppdomän och med administrationen av en sådan domän.

Domännamn utgör en beteckning för adressering av elektronisk kommunikation över Internet med användande av DNS. Ett domännamn kan bestå av olika namndelar åtskilda med en punkt, t.ex. www.naring.regeringen.se.

Definitionen av en *nationell toppdomän* ansluter till definitionen i artikel 3.3 i GAC:s principer. Lagens definition begränsas dock inte till den beteckning som följer av ISO-standarden SS-EN ISO 3166-1: Landsbeteckningar. Toppdomänen anges som den sista namndelen i ett domännamn.

Med *administratör* avses den som ansvarar för administrationen av en nationell toppdomän för Sverige. Vad som anses ingå i de olika delmomenten av administrationen av den nationella toppdomänen för Sverige beskrivs närmare i kapitel 9 i allmänmotiveringen.

Med *namnserver* avses en dator med namnserverprogramvara. Den fyller en servicefunktion i ett elektroniskt kommunikationsnät genom att lagra och distribuera zonfiler med information om domännamn samt ta emot och svara på domännamnsfrågor över ett sådant nät.

Administrationen av en nationell toppdomän

3 §

Administratören skall ha hemvist eller säte i Sverige.

Om administrationen av en nationell toppdomän helt eller delvis uppdras åt annan, skall det anmälas till den myndighet regeringen bestämmer (tillsynsmyndigheten).

Vad som föreskrivs i denna lag om administratören gäller även den till vilken det har uppdragits att helt eller delvis handha administrationen.

I *första stycket* föreskrivs en skyldighet för administratören av toppdomänen att ha hemvist eller säte i Sverige. Kravet motiveras bl.a. av att tillsynsverksamheten annars inte går att bedriva på ett effektivt sätt.

Administrationen av en nationell toppdomän är av sådant allmänt intresse att tillsynsmyndigheten bör informeras om någon getts i uppdrag av administratören att utföra någon del av administrationen av toppdomänen. I *andra stycket* föreskrivs därför att administratören av toppdomänen skall anmäla till tillsynsmyndigheten om administrationen till någon del uppdras åt annan. I anmälningsskyldigheten ligger inte något krav på att tillsynsmyndigheten skall godkänna upplåtelsen. Om det står klart att den till vilken uppdraget lämnats inte uppfyller t.ex. de tekniska krav som bör kunna ställas i dessa sammanhang, bör det åligga tillsynsmyndigheten att vidta åtgärder.

Av *tredje stycket* följer att vad som sägs i denna lag om administratören också gäller den som fått i uppdrag att utföra någon del av administrationen.

4 §

Administratören skall

1) *bedriva verksamheten under beaktande av allmänhetens intresse av effektiv Internetanvändning,*
2) *säkerställa en fungerande trafik mellan namnservrarna för toppdomänen och det globala kommunikationsnätet Internet,*
3) *tillse att domännamnen lagras i toppdomänens registerdatabas,*
4) *upprätthålla ett effektivt skydd av toppdomänens data, och*

5) *iaktta de internationella överenskommelser som Sverige har anslutit sig till eller bestämmelser antagna med stöd av Fördraget om upprättandet av Europeiska gemenskapen.*

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om på vilket sätt skyldigheter enligt första stycket skall fullgöras och om undantag från skyldigheterna.

I bestämmelsens *första stycke* föreskrivs vissa generella skyldigheter för den som administrerar den nationella toppdomänen för Sverige. Skyldigheterna knyter i stor utsträckning an till lagens ändamål att säkerställa en robust, effektiv och säker administration av toppdomänen. Frågor om lagens ändamål och driften av den nationella toppdomänen, exklusive namntilldelningen, har huvudsakligen behandlats i avsnitt 9.1.2 och 9.3 i allmänmotiveringen samt i kommentaren till 1 §. Driftsäkerhetsfrågorna har speciellt behandlats i avsnitt 9.3.2.

Första punkten berör bl.a. artikel 4.1 första meningen, 5.1, 5.3 och 9.1.2 i GAC:s principer. Det klargörs att administrationen av den nationella toppdomänen skall ske på ett sådant sätt att allmänhetens intresse av ett effektivt Internet så långt möjligt uppfylls.

Den i *andra punkten* uppställda skyldigheten att säkerställa en fungerande trafik mellan namnservrarna för toppdomänen och det globala kommunikationsnätet Internet avser huvudsakligen tillgängligheten av DNS-tjänsten. Skyldigheten innebär bl.a. att det skall finnas en permanent anslutningsmöjlighet avseende Internet Protocol (IP) till de namnservrar som tjänar den nationella toppdomänen och till den som administrerar toppdomänens registratur. Skyldigheten är inte absolut utan måste bedömas med hänsyn till vad som kan anses rimligt utifrån bl.a. teknisk genomförbarhet. Varje avbrott i anslutningsmöjligheten är alltså inte att se som ett åsidosättande av vad som åligger administratören av toppdomänen. Punkten motsvaras närmast av artikel 10.2.1 i GAC:s principer och har behandlats i avsnitt 9.3.2.

I *tredje punkten* klargörs administratörens grundläggande skyldighet att lagra registrerade domännamn i toppdomänens registerdatabas. Skyldigheten innebär att de poster som behövs för att uppnå funktionalitet i domännamnssystemet, t.ex. poster om de namnservrar som betjänar den underliggande huvuddomän till vilka trafik skall dirigeras, skall lagras i nämnda databas. Så sker genom att posterna sammanställs ur registerdatabasen till en zonfil som

lagras och kopieras till tjänande master- och slavservrar. Detta skall ske utan dröjsmål och med beaktande av de krav som i övrigt ställs på verksamheten. Bestämmelsen har närmast stöd i artiklarna 6.1, 6.2, 9.1.7, 10.2.1 och 10.2.5 i GAC:s principer.

Den i *fjärde punkten* uppställda skyldigheten avser att säkerställa skyddet för den nationella toppdomänens data, t.ex. skydd mot läsning, skrivning och borttagning. I skyldigheten ligger inte endast att skydda den information som finns lagrad i registerdatabasen utan även den information som distribueras till de namnservrar som betjänar toppdomänen. Bestämmelsen grundas närmast på artiklarna 9.1.7, 10.2.1 och 10.2.5 i GAC:s principer.

I *femte punkten* klargörs att administratören av den nationella toppdomänen måste beakta de internationella överenskommelser som Sverige har anslutit sig till eller bestämmelser antagna med stöd av Fördraget om upprättandet av Europeiska gemenskapen. Bestämmelsen motsvaras närmast av artikel 9.1.3 i GAC:s principer.

Genom *andra stycket* bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om på vilket sätt skyldigheter som uppställs i första stycket skall fullgöras och om undantag från dem. Föreskrifterna bör utformas med särskilt beaktande av ICANN:s riktlinjer (jfr artikel 9.1.7 i GAC:s principer).

5 §

Administratören skall fastställa och offentliggöra regler för tilldelning av domännamn under toppdomänen.

Regler för tilldelning av domännamn skall utformas med särskilt beaktande av

1) att förfarandet skall vara öppet och icke-diskriminerande,
2) skyddet för den personliga integriteten,
3) användarnas och andra allmänna intressen, samt
4) utvecklingen på Internetområdet.

Ansökningsavgift och årsavgift för ett domännamn skall vara skälig.

Bestämmelsens *första och andra stycken* innehåller dels en förpliktelse för administratören av den nationella toppdomänen för Sverige att fastställa och offentliggöra regler för tilldelning av domännamn under toppdomänen, dels en uppräkning av vilka intressen som skall beaktas vid fastställandet av regelverket.

Vissa av de punkter som skall beaktas vid fastställandet av regelverket följer redan av annan lag. Detta är exempelvis fallet med punkten 4 där det talas om skyddet för den personliga integriteten. I de fall integritetsaspekterna rör behandling av personuppgifter måste administratören följa de integritetsskyddande bestämmelser som följer av PUL. Att administratören skall beakta slutanvändarnas intressen innebär exempelvis att regelverket bör utformas på ett sätt som medger så många som möjligt att registrera domännamn under toppdomänen. I att iaktta användarnas intressen bör också ligga att administratören av toppdomänen bör reservera vissa ord. Detta bör bl.a. gälla kommunnamn och liknande beteckningar, men också sådana ord som kan användas i vilseledande syfte och som därför getts ett särskilt skydd i lag. Så är exempelvis fallet med vissa titlar, såsom advokat och läkare. Vid en bedömning av vilka ord som skall tas upp på en lista som reserverade bör man emellertid vara restriktiv, eftersom varje sådan åtgärd innebär ett avsteg från grundprincipen om icke-förprövning (se vidare i avsnitt 9.4.4).

Frågan om en avgift är skälig enligt *tredje stycket* skall bedömas utifrån enskildas ekonomiska förmåga att betala för ansökan om och innehav av ett eget domännamn. Syftet med bestämmelsen är att avgifterna inte skall hindra eller försvåra för privatpersoner att inneha egna domännamn under en nationell toppdomän (se vidare avsnitt 9.4.4).

6 §

Administratören skall föra ett allmänt tillgängligt register över beviljade domännamn samt upprätta säkerhetskopior av registerdata. En kopia av registret skall tillhandahållas tillsynsmyndigheten.

Registret skall innehålla uppgifter om:

1) domännamnet,
2) namn, postadress, telefonnummer och adress för elektronisk post till domännamnsinnehavaren och den som tekniskt administrerar domännamnet,
3) uppgifter om till domännamnet knutna namnservrar, samt
4) övrig teknisk information som behövs för att administrera domännamnet.

Uppgift enligt första stycket 2 får underlåtas att göras allmänt tillgänglig om särskilda skäl föreligger.

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om registerverksamhet och tillhandahållande av säkerhetskopia enligt första och andra stycket.

Bestämmelsen motsvarar närmast artikel 9.1.7 i GAC:s principer och har behandlats i avsnitt 9.3.3. Bestämmelsen utgör en särreglering i förhållande till PUL som i berörda delar ger vika för nu aktuell reglering.

Första stycket i bestämmelsen slår fast den grundläggande skyldigheten att föra ett register över beviljade domännamn. I skyldigheten ingår även att hålla registret allmänt tillgängligt. Grunden för denna skyldighet är att det vid behov snabbt och effektivt skall kunna skapas kontakt mellan t.ex. olika domännamnsinnehavare för att säkerställa Internets funktion och säkerhet. Som ett ytterligare led i säkerställandet av Internets funktion föreskrivs att säkerhetskopior, dvs. kopior av en fil eller andra data som sparas för att användas om originalet blir förstört, av registerdata skall upprättas. Vidare skall en kopia av registret, som en säkerhetsåtgärd, även tillhandahållas tillsynsmyndigheten för förvaring.

I *andra stycket* anges vilka registerdata som skall finnas med i registret. Frågan har behandlats i avsnitt 9.3.3.

För att undvika röjande av kontaktuppgifter som skall eller bör hållas hemliga, t.ex. telefonnummer eller skyddade adresser, innehåller *tredje stycket* en möjlighet till undantag från skyldigheten att göra uppgifterna tillgängliga för allmänheten.

De regler som närmare skall gälla för t.ex. tillhandahållande av kopia av det aktuella registret och för förvaring av säkerhetskopior på säker plats bör fastställas av regeringen eller tillsynsmyndigheten genom särskilda föreskrifter. I *fjärde stycket* lämnas ett sådant bemyndigande.

7 §

Om ansvaret för administrationen av en nationell toppdomän övergår till en annan administratör skall den tidigare administratören utan dröjsmål överföra registerdata som är nödvändiga för verksamheten till den nye administratören.

Om ansvaret för administrationen av en nationell toppdomän upphör utan att det finns någon ny administratör, skall tillsynsmyndigheten tillse att administratörens uppgifter utförs till dess en ny administratör finns.

Den som överför registerdata enligt första stycket har rätt till skälig ersättning.

För att säkerställa att driften av den nationella toppdomänen för Sverige inte försämras vid ett byte av administratör åläggs i *första stycket* den som upphör med verksamheten att föra över de registerdata som är nödvändiga för att administrationen skall kunna fortsätta. Bestämmelsen tar sin utgångspunkt i artikel 9.1.5 i GAC:s principer.

Genom bestämmelsen i *andra stycket* är det tillsynsmyndighetens uppgift att tillse att verksamheten med att administrera den nationella toppdomänen fullföljs till dess att en ny administratör finns.

Enligt *tredje stycket* har den som överför registerdata rätt till skälig ersättning. Ersättningen skall betalas av den till vilken överföringen av registerdata sker. I det fall tillsynsmyndigheten under en övergångsperiod skall ansvara för administrationen skall ersättningen följaktligen erläggas av myndigheten, som i sin tur har rätt till motsvarande ersättning av den till vilken administrationen slutligen överlåts.

Vid bestämmandet av ersättningen bör man först och främst beakta dels marknadsvärdet vid tidpunkten för överförandet av de registerdata som förpliktelsen avser, dels den ideella skada som kan uppkomma. Bestämmelsens utformning ger emellertid också möjlighet att låta ersättningen avse kompensation för t.ex. nedlagt arbete.

Om överenskommelse om ersättningens storlek inte kan träffas, får frågan avgöras av domstol. Skyldigheten att överföra registerdata gäller dock oberoende av om ersättningsfrågan är löst eller inte.

Tillsyn

8 §

Tillsynen skall säkerställa att lagen och föreskrifter som har meddelats med stöd av lagen efterlevs.

I bestämmelsen klargörs vilken uppgift tillsynsverksamheten skall tjäna. Det anges att syftet med denna är att säkerställa att

administratören av den nationella toppdomänen för Sverige efterlever lagen och de föreskrifter som har meddelats med stöd av lagen. Tillsynsverksamheten träffar till följd av regleringen i 3 § tredje stycket även den som på uppdrag av administratören, helt eller delvis, rent faktiskt administrerar toppdomänen. Tillsynsverksamheten har behandlats i avsnitt 9.6 i allmänmotiveringen.

9 §

Administratören skall på tillsynsmyndighetens begäran lämna den information och bereda tillgång till den utrustning och annat som behövs för tillsynen.

Tillsynsmyndigheten har rätt att för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av denna lag bedrivs.

I bestämmelsen, som har behandlats i avsnitt 9.6.2, ges de befogenheter som tillsynsmyndigheten måste ha för att kunna utföra sitt uppdrag. Tillsynsmyndighetens möjligheter att få nödvändig information om tillsynsobjektets verksamhet samt att få tillträde till områden, lokaler och andra utrymmen är grundläggande för en effektiv tillsyn.

Skyldigheten i *första stycket* att lämna information kan gälla såväl generell information som information i ett särskilt fall. Emellertid gäller informationsskyldigheten endast i den mån den behövs för tillsynsverksamheten, inbegripet den utvecklingsuppföljning som åvilar tillsynsmyndigheten enligt 10 § och omvärldsanalys. Skyldigheten att tillhandahålla utrustning och annat som behövs för tillsynen kan gälla sådan utrustning, t.ex. datorer, som förvaras på ett sådant sätt att tillsynen annars kan försvåras eller omöjliggöras, t.ex. i bostäder.

Rätten enligt *andra stycket* för tillsynsmyndigheten att få tillträde till områden, lokaler och andra utrymmen motsvaras av en skyldighet för administratören av toppdomänen att tillhandahålla begärt tillträde. Även om förhållandet inte uttrycks direkt i lagtexten skall det intrång som tillträdet innebär stå i proportion till behovet av åtgärden för tillsynsverksamhetens bedrivande.

10 §

Tillsynsmyndigheten skall övervaka utvecklingen av och nivån på ansökningsavgifter och avgifter för domännamnsinnehavare samt för kostnader för avregistreringsförfarande enligt 12 §.

Den ifrågavarande bestämmelsen har behandlats i avsnitt 9.4.4 och 9.5.3. Regleringen i paragrafen syftar till att säkerställa att domännamn och ett avregistreringsförfarande tillhandahålls till rimliga priser enligt 5 § tredje stycket och 12 § andra stycket. Uppgiften är speciellt viktig med hänsyn till den ökande andelen konsumenter bland domännamnsinnehavarna.

11 §

Tillsynsmyndigheten får meddela de förelägganden som behövs för efterlevnaden av denna lag eller föreskrifter som har meddelats med stöd av lagen.

Beslut om föreläggande får förenas med vite.

Bestämmelsen ger de maktbefogenheter som tillsynsmyndigheten behöver för att kunna bedriva en effektiv tillsynsverksamhet. Den har behandlats i allmänmotiveringen under avsnitt 9.6.2.

Enligt *första stycket* ges tillsynsmyndigheten rätt att genom föreläggande kräva åtgärder för att administratören av den nationella toppdomänen skall uppfylla de mål, krav och skyldigheter som följer av lagen eller föreskrifter meddelade med stöd av lagen.

Av *andra stycket* framgår att ett föreläggande enligt första stycket får förenas med vite.

Avregistrering och överföring av domännamn i särskilda fall

12 §

Administratören får efter ansökan av annan avregistrera ett domännamn, om det är uppenbart att innehavaren i ond tro registrerat eller använt domännamnet och denne inte har någon rätt till eller saknar berättigat intresse av den benämning som utgör domännamnet. I stället för avregistrering får domännamnet på särskild begäran överföras på annan innehavare.

För behandling av en ansökan enligt första stycket får administratören ta ut skälig avgift.

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om hur prövningen enligt första stycket skall ske.

Bestämmelsens *första stycke* överensstämmer i sak med artikel 9.1.6 i GAC:s principer och har behandlats närmare i avsnitt 9.5.3.

I *andra stycket* anges att administratören av den nationella toppdomänen för Sverige får ta ut avgifter i samband med avregistrerings- och överföringsförfarandet. Enligt 10 § i lagförslaget har tillsynsmyndigheten att övervaka utvecklingen av nivån för sådana avgifter. Eftersom det regelverk för namntilldelning som trädde i kraft i april 2003 tillåter både juridiska och fysiska personer att registrera domännamn under toppdomänen bör de avgifter som tas ut i samband med avregistrerings- och överföringsförfarandet differentieras. Detta för att det skall vara ekonomiskt möjligt för samtliga som kan registrera domännamn under domänen att använda sig av det förfarande som erbjuds. En rimlig kostnad i dagsläget är enligt utredningen för en tvist som inleds av en juridisk person 1 000 kr, medan en tvist som inleds av en fysisk person bör föranleda en avgift om 500 kr.

Tillsynsavgift

13 §

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får föreskriva om skyldighet för administratören att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Uttaget av tillsynsavgift har berörts i avsnitt 9.6.2. Det skall täcka de kostnader som är direkt relaterade till kontrollen av lagens efterlevnad. Det kan också finnas skäl att låta kostnader som på annat sätt är relaterade till tillsynsverksamheten täckas helt eller till del av nu aktuell avgift. Någon förändring i förhållande till vad som gäller idag beträffande anslagsfinansierad verksamhet är dock inte avsedd.

Verkställighet

14 §

Tillsynsmyndigheten har rätt att få verkställighet hos kronofogdemyndigheten av beslut som avser åtgärder enligt denna lag. Därvid gäller bestämmelserna i utsökningsbalken om sådan verkställighet som avses i 16 kap. 10 § den balken.

Bestämmelsen har behandlats i den allmänna motiveringen, se avsnitt 9.6.2. Den ger tillsynsmyndigheten möjlighet att få verkställighet av beslut som avser åtgärder enligt lagen. De bestämmelser i utsökningsbalken som därvid skall tillämpas avser frågor om verkställighet av förpliktelser som inte avser betalningsskyldighet samt frågor om verkställighet av beslut om kvarstad eller andra säkerhetsåtgärder.

Verksamhet i krig och kris

15 §

Är Sverige i krig eller krigsfara eller råder det sådana utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara, får regeringen meddela de föreskrifter om administrationen av en nationella toppdomän som behövs med hänsyn till landets försvar eller säkerhet i övrigt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om den fredstida planeringen för totalförsvarets behov av adressering med användande av domännamnssystemet under sådana förhållanden som anges i första stycket.

Paragrafen gör det möjligt för regeringen att enligt 13 kap. 6 § regeringsformen under krig och vissa därmed likartade förhållanden samt i fredstid meddela föreskrifter enligt vad som framgår av lagtexten och som annars skulle meddelas i lag.

Överklagande

16 §

Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen regleras rätten att överklaga beslut som tillsynsmyndigheten har meddelat enligt lagen och enligt föreskrifter som meddelats med stöd av lagen.

Särskilt yttrande

Särskilt yttrande av Kjell Skoglund

Internet har utvecklats till en idag mycket betydelsefull men ännu inte samhällskritisk resurs. Det framgår inte minst av de rapporter från IT-kommissionen som anges i betänkandet.

Trendmässigt finns ett ökat offentligt intresse för administrationen av landstoppdomänerna. EU-kommissionen har exempelvis uppmanat medlemsstaterna att genomföra GAC:s principer på ett lämpligt sätt i den mån de avser regeringars förhållande till ICANN och sina nationella toppdomänregister.

Domännamnssystemet är redan idag som en helhet en kritisk resurs för hela den globala Internetanvändningen. Däremot är inte toppdomänen *se* i sig en kritisk resurs på samma sätt. Det finns idag ett stort antal toppdomäner att tillgå. Sålunda är det min bedömning att denna "marknad" inte är i behov av någon särskild tillsyn från staten, utöver vad som kan sägas gälla redan idag.

Redan idag har PTS att bevaka hanteringen av den svenska toppdomänen *se*. Samverkan mellan PTS och II Stiftelsen för att åstadkomma ett robust Internet i Sverige – inbegripet hanteringen av domännamnssystemet – tycks utveckla sig i en konstruktiv riktning, se bl.a. PTS senaste rapport om robusthet. Detta arbete täcker i sig in en del av vad som ryms under begreppet administration såsom det avgränsats av utredningen.

Enligt min uppfattning fungerar dagens system för administration av den svenska toppdomänen *se*. Några anledningar – såsom tycks ha förelegat i Norge och Finland – för att förändra detta anser jag inte föreligger.

Kommittédirektiv

Ny lagstiftning och myndighetsorganisation inom området för elektronisk kommunikation text

Dir. 2001:32

Beslut vid regeringssammanträde den 19 april 2001.

Sammanfattning av uppdraget

En särskild utredare skall se över de politiska målen inom området för elektronisk kommunikation. Arbetet skall bedrivas mot bakgrund av såväl den tekniska och marknadsmässiga utveckling som skett inomområdet som de rättsakter som kommer att antas inom Europeiska unionen.

Utredaren skall analysera lagstiftningen inom området och föreslå sådan ny lagstiftning som behövs, med inriktning på en horisontell och samordnad reglering av elektronisk kommunikationsinfrastruktur och elektroniska kommunikationstjänster. Uppdraget omfattar inte förslag till grundlagsändringar.

Utredaren skall också överväga och ge förslag på den myndighetsstruktur som är lämplig med anledning av de förslag till lagstiftning som utredaren lägger fram, erfarenheterna av nuvarande organisation och den tekniska utveckling som har skett och kan förutses i framtiden samt föreslå den författningsreglering som behövs för ändamålet.

Uppdraget omfattar följande frågor:

- Utredaren skall genomföra en fullständig översyn av telelagen (1993:597) och lagen (1993:599) om radiokommunikation samt de nu gällande politiska målen för dessa. Utgångspunkten är i huvudsak de EG-direktiv och det EG-beslut som kommer att antas inom detta område, som en följd av 1999 års kommunikationsöversyn. I den mån radio- och TV-lagen (1996:844) påverkas av dessa skall även denna bli föremål för översyn i detta avseende.
- Utredaren skall lämna förslag till hur EG-rättsakterna skall genomföras i svensk lagstiftning.

- Utredaren skall utöver nämnda lagar kartlägga och analysera övrig lagstiftning inom området för elektronisk kommunikation och överväga om det finns behov av en samordning samt föreslå erforderliga förändringar med inriktning på en samlad lagstiftning.
- Utredaren skall beskriva nuvarande myndighetsstruktur på området och de samarbetsformer som finns mellan myndigheterna samt föreslå de förändringar i organisationen som är påkallade.
- Utredaren skall lämna de författningsförslag som anses nödvändiga för att möjliggöra statlig tillsyn av de principer för administration av nationella toppdomäner för adressering på Internet som utarbetats av den mellanstatliga rådgivande kommittén (GAC).

Uppdraget skall redovisas senast den 1 april 2002.

Bakgrund

De elektroniska kommunikationernas betydelse i samhället

Väl fungerande elektroniska kommunikationer är en fundamental förutsättning för det moderna samhället. I och med att informationsutbytet och internationaliseringen har ökat och i takt med informationsteknikens utbredning inom flera samhällssektorer, har elektronisk kommunikation blivit allt viktigare för ekonomins tillväxt, näringslivets utveckling och viktiga samhällsfunktioner. Sverige är idag ett av världens ledande länder när det gäller användningen av informationsteknik och telekommunikationer. Det är angeläget att vi kan behålla och vidareutveckla denna framskjutna position. En förutsättning för detta är ett regelverk och en ändamålsenlig myndighetsstruktur som kan ta tillvara den utvecklingskraft som finns inom sektorn för elektroniska kommunikationer.

Det finns ett behov av att se över lagstiftningen, de politiska målen och myndighetsstrukturen med anledning av den tekniska och marknadsmässiga utvecklingen samt nya EG-direktiv och EG-beslut som kommer att antas under det närmaste året.

Nu gällande politiska mål

Elektronisk kommunikation behandlas för närvarande i första hand inom politikområdena telepolitik, IT-politik och mediepolitik. Nuvarande telepolitiska mål har sin grund i 1988 års telepolitiska beslut (prop. 1987/88:118, bet. 1987/88:TU28, rskr. 1987/88:402) och reviderades senast 1996 (prop. 1996/97:61, bet. 1996/97:TU5, rskr.1996/97:201). Det övergripande målet är att enskilda och myndigheter skall ha tillgång till effektiva telekommunikationer till lägsta möjliga samhällsekonomiska kostnad.

Nyligen har ett IT-politiskt mål fastställts av riksdagen (prop.1999/2000:86, bet. 1999/2000:TU9, rskr. 1999/2000:256). Målet är att Sverige som första land skall vara ett informationssamhälle för alla. Målet för mediepolitiken fastställdes av riksdagen i slutet av år 2000(prop. 2000/01:1, bet. 2000/01:KrU:1, rskr. 2000/01:59). Målet är att stödja yttrandefrihet, mångfald, massmediernas oberoende och tillgänglighet samt att motverka skadliga inslag i massmedierna.

Nuvarande lagstiftning på området för elektronisk kommunikation

Telelagen och lagen om radiokommunikation

Telelagen och lagen om radiokommunikation trädde i kraft den 1 juli 1993. Telelagen innehåller bestämmelser om televerksamhet. Lagen anger förutsättningar för bl.a. tillståndsplikt, tillståndsprövning, tillståndsvillkor, taxor, samtrafik, nummerplanering och tillsyn. Lagen om radiokommunikation syftar till att främja ett effektivt nyttjande av möjligheterna till radiokommunikationer och andra användningar av radiovågor. Lagen innehåller huvudsakligen regler om rätten att använda radiosändare. En översyn av telelagen genomfördes 1996. Lagen om radiokommunikation har inte varit föremål för någon översyn.

Radio- och TV-lagen

Radio- och TV-lagen innehåller föreskrifter om sändningar av ljudradio- och TV-program som är riktade till allmänheten och avsedda att tas emot med tekniska hjälpmedel. När det gäller

distributionen av vissa sådana sändningar ger lagen regeringen rätt att ange villkor i fråga om bl.a. sändningarnas geografiska räckvidd och att tillståndshavare skall samarbeta i tekniska frågor. I lagen finns även föreskrifter om vidaresändningar i kabelnät av vissa TV-program.

Marknadsmässig och teknisk utveckling

Marknaden för elektroniska kommunikationstjänster är mycket dynamisk. Konkurrensen mellan aktörerna och den tekniska utvecklingen driver fram nya och bättre tjänster och varor. Fler aktörer på marknaden sätter också en press på priserna och tvingar fram nytänkande.

Den traditionella telefonin har vidareutvecklats och sättet att kommunicera sker genom allt mer avancerade former av informationsteknik. Drivkrafterna i denna utveckling är särskilt användningen av Internet samt konvergensen. Med konvergens avses huvudsakligen att den tekniska utvecklingen, framför allt den digitala tekniken, minskar skillnaderna mellan området för privat kommunikation och massmedieområdet. Text, ljud, bild och data kan hanteras samtidigt och förmedlas genom flera former av distributionssystem. Detta leder till ett närmande mellan olika nät(t.ex. nät för telefoni, data och television), tjänster (kommunikationstjänster och innehållstjänster) och apparater (t.ex. telefoner och TV-mottagare). Det är i denna miljö som nya användningsområden och tillämpningar av informationsteknik växer fram i snabb takt.

Lagstiftningen och de politiska målen inom området för elektronisk kommunikation måste nu ses över i ljuset av denna utveckling för att inte riskera att bli föråldrade.

EG-direktiven m.m.

Telekommunikation ansågs länge vara en statlig uppgift. I de flesta medlemsstater inom Europeiska unionen var tillhandahållandet av infrastruktur och teletjänster förbehållet en statlig myndighet eller ett statligt ägt bolag. Under 1990-talet antogs emellertid en rad direktiv och beslut som successivt liberaliserade och harmoniserade telemarknaden inom Europeiska gemenskapen. Det samlade

regelverket på området består i dag av ett tjugotal direktiv och beslut. Dessa rättsakter är i huvudsak genomförda i telelagen och föreskrifter meddelade med stöd av lagen.

EG-kommissionen inledde hösten 1999 en översyn av regelverket och antog den 12 juli 2000 ett förslag till nytt regelverk för elektroniska kommunikationer bestående av följande direktiv: Förslag till Europaparlamentets och rådets direktiv om

- ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, KOM (2000) 393 slutlig (ramdirektivet),
- auktorisation för elektroniska kommunikationsnät och kommunikationstjänster, KOM (2000) 386 slutlig (auktorisationsdirektivet),
- tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande utrustning, KOM (2000) 384 slutlig (tillträdesdirektivet),
- samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, KOM (2000) 392 slutlig (USO-direktivet),
- behandling av personuppgifter och skydd för privatlivet inom sektorn för elektronisk kommunikation, KOM (2000) 385 slutlig (komdataskyddsdirektivet).

Den 12 juli 2000 antog kommissionen också ett förslag till Europaparlamentets och rådets beslut om ett regelverk för radiospektrumpolitiken inom Europeiska unionen (KOM (2000) 407 slutlig).

Regelverket antas enligt det s.k. medbestämmandeförfarandet (artikel 251 i Romfördraget). Behandlingen av rättsakterna, som enligt kommissionens förslag föreslås träda i kraft den 1 januari 2002, pågår för närvarande i Europaparlamentet och rådet.

Kommissionen avser dessutom att ersätta det nu gällande direktivet om konkurrens på marknaderna för teletjänster (90/388/EG, senast ändrat genom direktiv 1999/64/EG), med ett nytt direktiv om konkurrens på marknaderna för elektroniska kommunikationstjänster.

Rättsakterna inrättar ett harmoniserat regelverk för alla former av elektroniska kommunikationsnät, inklusive Internet (IP-baserade globala datanät), rundradionät och kabel-TV-nät, samt av elektroniska kommunikationstjänster. I det senare begreppet ingår dock inte tillhandahållande av innehåll eller utövande av

redaktionellt ansvar över innehåll som överförs med hjälp av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Regelverket påverkar inte nationella åtgärder som motiveras av allmänintresse, särskilt vad avser innehållsreglering och mediepolitik, under förutsättning att sådana åtgärder är i enlighet med EG-rätten.

Mediepolitiska mål och innehållsreglering i allmänhet kan således utformas av medlemsstaterna. När respektive medlemsstat skall uppnå de mediepolitiska målen får det dock inte uppstå konflikter med EG:s regelverk när det gäller infrastrukturen för elektronisk kommunikation.

Vissa utredningar av intresse

Konvergensutredningen

I konvergensutredningens betänkande Konvergens och förändring (SOU 1999:55) konstateras att konvergensutvecklingen med sammansmältning av olika medieformer och framväxten av helt nya tjänster medför olika gränsdragnings- och tolkningsproblem vid tillämpningen av gällande rätt. Dessa problem kan, enligt utredningen, framför allt hänföras till de begrepp, definitioner och avgränsningar som präglar utformningen av yttrandefrihetsgrundlagen (YGL), radio- och TV-lagen samt telelagen. Detta kan i sin tur medföra oönskade konsekvenser för såväl utvecklingen av nya tjänster, produkter och infrastrukturella lösningar som möjligheten att uppfylla tele- och mediepolitiska målsättningar. Utredningen anser därför att det finns ett behov av samordning av den aktuella lagstiftningen, vilket framför allt avser relationen mellan å ena sidan telelagen och å andra sidan YGL och radio- och TV-lagen. Hänsyn måste enligt utredningen tas till de begränsningar i möjligheten att lagstifta som i olika avseenden följer av överordnade regler och internationella förpliktelser. Det handlar främst om de begränsningar som följer av YGL och om Sveriges förpliktelser enligt EG-rätten samt, i fråga om användningen av radiofrekvenser, den internationella telekonventionen och radioreglementet.

Mediegrundlagsutredningen

Mediegrundlagsutredningen överlämnade den 29 mars 2001 betänkandet Yttrandefrihetsgrundlagen och Internet (SOU 2001:28). I betänkandet analyserar utredningen behovet av och förutsättningarna för en mer teknikneutral grundlagsreglering av yttrandefriheten. Utredningen föreslår att den nuvarande s.k. databasregeln i 1 kap. 9 § YGL utvidgas så att den omfattar också andra än massmedieföretag. För dessa andra införs en möjlighet att genom utgivningsbevis få ett frivilligt grundlagsskydd. Databasregeln föreslås omfatta även direktsändning på begäran. Nuvarande undantagsregel från etableringsfriheten i 3 kap. 1 § YGL utvidgas så att det inte finns hinder för regler som innebär dels en skyldighet för nätinnehavare att upplåta utrymme i nätet för andra överföringar än sådana som omfattas av grundlagen i den utsträckning det behövs med hänsyn till intresset av konkurrens för sådana tjänster i nätet, dels en skyldighet för nätinnehavare att tillförsäkra mottagarkretsen inflytande över programvalet.

Utredningen om översyn av radio- och TV-lagen m.m.

Utredningen om översyn av radio- och TV-lagen m.m. har i uppdrag att analysera och överväga behovet av ändringar i framför allt radio- och TV-lagen och lagen (1989:41) om TV-avgift. Utredningsuppdraget omfattar frågor om bl.a. jurisdiktion, tillämplighet av tillståndsvillkor på vissa sändningar samt skydd av barn mot olämpligt programinnehåll. Den del av uppdraget som gäller skydd av barn mot olämpligt programinnehåll skall redovisas före utgången av oktober 2001 medan uppdraget i övrigt skall vara slutfört före utgången av maj 2002.

Uppdraget

En särskild utredare skall utreda behovet av lagstiftning inom området för elektronisk kommunikation. Detta begrepp används ofta – bl.a. i kommissionens meddelande som föregick de ovan redovisade förslagen till EG-direktiv (KOM (1999) 539) – som en samlande benämning på den verksamhet som bedrivs inom det nya område som växer fram mot bakgrund bl.a. av konvergensutvecklingen och Internet. Utredaren skall beskriva detta område

och den tekniska och ekonomiska utveckling som skett under de senaste åren.

Gränsdragningen mellan å ena sidan sektorsspecifik lagstiftning inom berörda områden och å andra sidan de generella konkurrensreglerna skall belysas.

Utredaren skall vid uppdragets genomförande särskilt uppmärksamma och beakta att det föreslagna EG-rättsliga regelverket är tillämpligt även på IP-baserad elektronisk kommunikation.

Översyn av vissa politiska mål

Utredaren skall analysera de telepolitiska målen och de syften som ligger till grund för lagen om radiokommunikation. Utredaren skall även bedöma om dessa mål och syften är ändamålsenliga mot bakgrund av den marknadsmässiga och tekniska utvecklingen och den lagstiftning som utredaren föreslår samt föreslå de ändringar som behövs. I detta ingår även att analysera hur de mediepolitiska målen kan uppnås med beaktande av det nya EG-rättsliga regelverket. Någon översyn av de mediepolitiska målen skall däremot inte göras.

Utgångspunkten skall vara att en samordning skall ske mellan de telepolitiska målen och det IT-politiska målet. Utredaren skall också ange hur dessa politiska mål kan uppnås och särskilt beskriva statens roll i förhållande till marknaden i detta sammanhang.

Ny lagstiftning inom området för elektronisk kommunikation

Utredaren skall utifrån en redovisning och utvärdering av de erfarenheter som vunnits av tillämpningen genomföra en fullständig översyn av telelagen och lagen om radiokommunikation. En utgångspunkt är de förändringar som utredaren föreslår av de politiska målen inom området för elektronisk kommunikation. En annan viktig utgångspunkt i detta arbete är de nya EG-direktiv och EG-beslut som kommer att antas. Utredaren skall därvid följa behandlingen i rådet och Europaparlamentet av kommissionens förslag på området.

Ett EG-direktiv är bindande endast i fråga om det resultat som skall uppnås. Medlemsstaterna får själva välja form och metod för detta. Utredaren skall med beaktande av svensk lagstiftnings-

tradition föreslå den lagstiftning som är nödvändig för att genomföra de nya direktiven och beslutet om radiospektrumpolitiken. I den mån radio- och TV-lagen påverkas av de nya EG-direktivens regler om infrastruktur för elektronisk kommunikation skall även denna bli föremål för översyn i detta avseende.

Samordning av lagstiftning inom området för elektronisk kommunikation

Utredaren skall utöver en översyn av telelagen och lagen om radiokommunikation också kartlägga övrig lagstiftning som avser elektronisk kommunikation, bl.a. radio- och TV-lagen, lagen (2000:832) om kvalificerade elektroniska signaturer, lagen (2000:121) om radio- och teleterminalutrustning samt lagstiftning som genomför Europaparlamentets och rådets direktiv 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (EGT L 178, 17.7 2000, s. 1, Celex 32001L0031). Departementspromemorian E-handelsdirektivet (Ds 2001:13) innehåller förslag till sådan lagstiftning. Promemorian remissbehandlas för närvarande.

Utredaren skall överväga om nuvarande författningsstruktur på området är ändamålsenlig och i vilken utsträckning en systematisk samordning bör ske. I sitt arbete skall utredaren bl.a. vägledas av de slutsatser om behovet av samordning av lagstiftningen till följd av konvergensutvecklingen som redovisas i Konvergensutredningens betänkande. Detta innebär att utredningsarbetet skall inriktas mot en horisontell och samordnad reglering av elektronisk kommunikationsinfrastruktur och elektroniska kommunikationstjänster. En sådan inriktning ligger också väl i linje med de föreslagna EG-direktiven. Utredaren skall föreslå de förändringar av författningsstrukturen på området som övervägandena föranleder med inriktning på en samlad lagstiftning inom området. Syftet är att skapa en modern, teknikneutral och framtidsanpassad lagstiftning.

Myndighetsfrågor

Flera myndigheter har uppgifter inom området för elektronisk kommunikation, främst Post- och telestyrelsen och Radio- och TV-verket, men även bl.a. Konsumentverket, Konkurrensverket,

Riksarkivet och IT-kommissionen (K 1998:04). Utredaren skall beskriva den nuvarande myndighetsstrukturen och samarbetsformerna mellan myndigheterna. Därvid skall även erfarenheterna av den nuvarande organisationen redovisas och utvärderas. Utredaren skall överväga om nuvarande organisation är lämplig mot bakgrund av dessa erfarenheter, den tekniska utvecklingen, de överväganden som gjorts om statens uppgifter och den lagstiftning som utredaren föreslår. Utredaren skall föreslå de förändringar i myndighetsstrukturen och samarbetsformerna som är nödvändiga med anledning av dessa överväganden samt sådana förslag till författningsändringar som skulle bli nödvändiga för att åstadkomma en förändrad myndighetsstruktur.

Förslagens ekonomiska konsekvenser skall analyseras och redovisas.

Administrationen av toppdomänen punkt-se

En närliggande fråga är administrationen av domännamn under den nationella toppdomänen punkt-se. Vissa aspekter av Internet täcks in av de föreslagna EG-direktiven. De berör dock inte frågan om administration av domännamnssystemet. På internationell nivå har den mellanstatliga rådgivande kommittén (GAC) till Internet Corporation on Assigned Names and Numbers (ICANN) den 23 februari 2001 utarbetat principer för delegering och administration av nationella toppdomäner. I Domännamnsutredningens betänkande (SOU 2000:30) finns en beskrivning av domännamnssystemet.

Domännamnsutredningen har föreslagit att Sverige inför en avtalsmodell motsvarande den som GAC har föreslagit för delegering av ansvaret för de nationella toppdomänerna. Sedan Domännamnsutredningens betänkande lämnades har kommissionen i meddelandet KOM(2000)202 den 4 juli 2000 uppmanat medlemsstaterna att genomföra GAC:s principer på ett lämpligt sätt i den mån de avser regeringars förhållande till ICANN och till sina nationella landsdomänregister. Europeiska unionens råd uppmanade den 3 oktober 2000 medlemsstaterna att med beaktande av nationella bestämmelser genomföra GAC:s principer för delegering och administration av nationella toppdomäner. Utredaren skall beskriva och utvärdera tillämpningen av GAC:s principer i dag för

den nationella toppdomänen punkt-se. Utredaren skall undersöka möjligheterna att genomföra principerna, särskilt artikel 5 som rör statens roll, genom en offentligrättslig reglering och lämna de författningsförslag som anses nödvändiga för att möjliggöra statlig tillsyn av principernas efterlevnad. Förslagens ekonomiska konsekvenser skall analyseras och redovisas.

Övrigt

Utredaren skall ha stor frihet att ta upp de ytterligare frågor som denne anser behöver övervägas inom ramen för uppdraget. Det ingår dock inte i uppdraget att föreslå grundlagsändringar.

Utredningsarbetet

Utredaren skall samråda med representanter för organisationer och företag inom området samt med berörda myndigheter. Om utredaren föreslår ändringar i radio- och TV-lagen skall förslagen utformas i samråd med utredningen om översyn av radio- och TV-lagen m.m.

Utredaren skall även beakta konsekvenserna av föreslagen lagstiftning för små företags villkor, i enlighet med 15 § kommittéförordningen (1998:1474). Utredaren skall härvid samråda med Näringslivets Nämnd för Regelgranskning.

Utredaren skall beakta Mediegrundlagsutredningens betänkande (SOU 2001:28) och den vidare beredningen av det.

Utredaren skall beakta den vidare beredningen av departementspromemorian. Effektivare tvistlösning på teleområdet (Ds 2000:56) samt Post- och telestyrelsens skrivelse den 1 september 2000 Upplysning om teleadresser.

Sårbarhets- och säkerhetsutredningen (Fö 1999:04) skall redovisa sitt arbete den 1 maj 2001. Utredaren skall inom ramen för sitt uppdrag beakta utredningens betänkande och den vidare beredningen av det.

Regeringen uppdrog åt Post- och telestyrelsen i dess regleringsbrev för år 2001 att utreda vissa frågor för att säkerställa driften av Internet i Sverige. Uppdragen skall redovisas senast den 1 oktober 2001. Utredaren skall beakta myndighetens skrivelse med redovisning av uppdragen.

Utredaren skall också beakta Bredbandsutredningens betänkande (SOU 2000:111).

Utredaren skall redovisa sitt uppdrag senast den 1 april 2002.

(Näringsdepartementet)

Principles for the Delegation and Administration of Country Code Top Level Domains

1. Preamble

In the five years since the issuance of RFC 1591, the Internet has evolved from a tool reserved for computer and networking research, to a global medium for commerce, education, and communication. The new realities of the Internet, including its increased importance as a vehicle for national economic growth, and the expanding and more diverse nature of the Internet community necessitated evolution in the traditional means of managing and administering Internet technical functions.

As a result, DNS functions, including the administration of the DNS root server system, the development of policies for the registration and allocation of domain names, the coordination of Internet Protocols, and the delegation of Internet Protocol numbers are becoming more clearly delineated and formalised through the ICANN process. Similarly, the procedures and framework of accountability for delegation and administration of ccTLDs need to evolve into a more robust, certain, and reliable system as well.

While evolution is needed, the principle of RFC 1591 remains sound: the manager of a ccTLD performs a public service on behalf of the relevant local community and as such the designated manager has a duty to serve this community. The designated manager also has a responsibility to the global Internet community. By ‘global Internet community' we do not mean any specific legal or international entity, but rather we interpret the term to refer to all of those who are affected by, now or in the future, the operation of the relevant TLD, because such operation may impinge on more than one jurisdiction and affect the interests of individuals and entities from both within the relevant country or territory and elsewhere. This is our interpretation of the meaning of ‘global Internet community' as it is used in RFC 1591.

2. Objective of this Document

The objective of this document is to suggest principles that will assist in the development of best practice for the delegation and administration of ccTLDs. These principles are intended to contribute to the development of models of:

- a communication between the relevant government or public authority and ICANN;
- a communication between ICANN and the delegee; and
- a communication between the relevant government or public authority and the delegee.

3. Definitions

For the purposes of this document, the following definitions apply:

3.1 'Alternative Dispute Resolution' (or 'ADR') means any system of resolving a dispute other than by court litigation, and includes arbitration, mediation, conciliation and processes of administrative dispute resolution.

3.2 'Communication' should include a law, regulation, agreement, document, contract, memorandum of understanding, or any other written instrument, as appropriate.

3.3 'Country code top level domain' or 'ccTLD' means a domain in the top level of the global domain name system assigned according to the two-letter codes in the ISO 3166-1 standard, 'Codes for the Representation of Names of Countries and Their Subdivisions.'

3.4 'Delegation' means delegation by ICANN/IANA of responsibility for administration of a TLD in the DNS root.

3.5 'Delegee' means the organisation,enterprise or individual designated by the relevant government or public authority to exercise the public trust function of a ccTLD and consequently recognised through a communication between ICANN and the designated entity for that purpose. The delegee for a ccTLD may be the relevant government or public authority itself or an oversight body designated by the relevant government or public

authority, inasmuch as the administrative and management functions for a ccTLD may be contracted out by the delegee to another party and hence not performed by the delegee itself.

3.6 'Designation' means designation by the relevant government or public authority of the delegee.

3.7 'DNS' means domain name system.

3.8 'ICANN' means the Internet Corporation for Assigned Names and Numbers.

3.9 'Relevant government or public authority' means relevant national government or public authority of a distinct economy as recognised in international fora as those terms are used in the ICANN Bylaws and GAC Operating Principles.

3.10 'Relevant local community' means the local community in the context of the ISO 3166-1 code. This definition is specific to the purposes identified in this document and not broader.

3.11 'Top Level Domain' or 'TLD' means a domain in the top level of the global domain name system.

4. Role of Delegee

4.1 The delegee of a ccTLD is a trustee for the delegated domain, and has a duty to serve the residents of the relevant country or territory in the context of ISO 3166-1, as well as the global Internet community (as that term is interpreted in the Preamble to this document). Its policy role should be distinguished from the management, administration and marketing of the ccTLD. These functions may be performed by the same or different entities. However the delegation itself cannot be sub-contracted, sub-licensed or otherwise traded without the agreement of the relevant government or public authority and ICANN.

4.2 No private intellectual or other property rights should inhere in the ccTLD itself, nor accrue to the delegee as the result of

delegation or to any entity as a result of the management, administration or marketing of the ccTLD.

4.3 Tradable goods and services may arise in the performance of other management and administrative functions attached to the ccTLD.

4.4 The delegee should recognise that ultimate public policy authority over the relevant ccTLD rests with the relevant government or public authority.

4.5 The delegee should work cooperatively with the relevant government or public authority of the country or territory for which the ccTLD has been established, within the framework and public policy objectives of such relevant government or public authority.

4.6 The delegee, and the delegee's administrative contact, should be resident or incorporated in the territory and/or jurisdiction of the relevant government or public authority. Where the delegee, administrative contact or technical contact are not resident or incorporated in the territory and/or jurisdiction of the relevant government or public authority, it should nevertheless operate in a way that is consistent with the laws and public policy of that relevant government or public authority.

5. Role of Government or Public Authority

5.1 The relevant government or public authority ultimately represents the interests of the people of the country or territory for which the ccTLD has been delegated. Accordingly, the role of the relevant government or public authority is to ensure that the ccTLD is being administered in the public interest, whilst taking into consideration issues of public policy and relevant law and regulation.

5.2 Governments or public authorities have responsibility for public policy objectives such as: transparency and non-discriminatory practices; greater choice, lower prices and better services for all categories of users; respect for personal privacy; and

consumer protection issues. Considering their responsibility to protect these interests, governments or public authorities maintain ultimate policy authority over their respective ccTLDs and should ensure that they are operated in conformity with domestic public policy objectives, laws and regulations, and international law and applicable international conventions.

5.3 It is recalled that the Governmental Advisory Committee (GAC) to ICANN has previously adopted the general principle that the Internet naming system is a public resource in the sense that its functions must be administered in the public or common interest.

5.4 The relevant government or public authority should ensure that DNS registration in the ccTLD benefits from effective and fair condition of competition, at appropriate levels and scale of activity.

5.5 To give effect to governments' or public authorities' public policy interests, governments or public authorities should ensure that the terms outlined in Clause 9 are included in their communications with delegees.

5.6 In making a designation for a delegee, the government or public authority should take into consideration the importance of long term stability in the administration and management of the ccTLD and in the DNS. In most cases, such stability may be best served through the designation of an organisation or an enterprise rather than a specific individual.

6. Role of ICAAN

6.1 A primary function of ICANN is to establish, disseminate, and oversee implementation of the technical standards and practices that relate to the operation of the global DNS. In this capacity, ICANN administers a range of technical Internet management functions, including:

- establishment of policy for IP number block allocation;
- administration of the authoritative root server system;
- creation of policy for determining the circumstances under which new TLDs would be added to the root system;

- coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet; and
- other activities necessary to coordinate specified DNS administration functions.

6.2 Specifically in relation to the administration and operation of ccTLDs, ICANN's role is to develop and implement policies that fulfil the provisions of Clause 10 below.

7. Principles relating to Delegations

7.1 Where a communication between the relevant government or public authority and the delegee is in place, when ICANN is notified by the relevant government or public authority that the delegee has contravened the terms of the communication, or the term of the designation has expired, ICANN should act with the utmost promptness to reassign the delegation in coordination with the relevant government or public authority.

7.2 Notwithstanding the urgent need for a communication-based regime for ccTLD designation, delegation and administration, in the absence of such communication between the relevant government or public authority and the administrator of the ccTLD, ICANN should, upon the tendering of evidence by such government or public authority that the administrator does not have the support of the relevant local community and of the relevant government or public authority, or has breached and failed to remedy other material provisions of RFC 1591, act with the utmost promptness to reassign the delegation in coordination with the relevant government or public authority.

7.3 When ICANN notifies the relevant government or public authority that the ccTLD is being operated in a manner that threatens the stability of the DNS or of the Internet, or has otherwise breached and failed to remedy other material provisions of the communication between ICANN and the delegee, as outlined in Clause 10, the relevant government or public authority should cooperate with ICANN to remedy this situation or effect the reassignment of the delegation for the ccTLD.

7.4 With respect to future delegations or reassignment of delegations, ICANN should delegate the administration of a ccTLD only to an organisation, enterprise or individual that has been designated by the relevant government or public authority.

7.5 Delegees should enjoy, in the execution of their responsibilities, the appropriate rights under applicable law, and should not be subject to discriminatory or arbitrary practices, policies or procedures from ICANN or the relevant government or public authority. In the event of a reassignment of delegation, registrants in the ccTLD should be afforded continued name resolution, or a reasonable period in which to transfer to another TLD.

8. Principles concerning the Communication between the relevant Government or Public Authority and ICAAN

8.1 The communication between the relevant government or public authority and ICANN, as outlined in Clause 2, should include a designated point of contact within the relevant government or public authority, as well as the name and contact details of the recognised delegee and duration of this recognition. Either as part of this communication, or through a subsequent communication, the relevant government or public authority should copy to ICANN any communication established between it and the delegee, setting forth the terms and conditions of the designation and/or concerning the execution of the delegee's role and the management of the delegation.

8.2 The relevant government or public authority should communicate to ICANN how it will require the delegee to abide by the terms and conditions outlined in Clause 9 below.

8.3 Recognising ICANN's responsibilities to achieve consensus in the creation of any new generic TLDs, ICANN should avoid, in the creation of new generic TLDs, well known and famous country, territory or place names; well known and famous country, territory or regional language or people descriptions; or ISO

639 Codes for representation of languages unless in agreement with the relevant governments or public authorities.

9. Principles concerning the Communication between the relevant Government or Public Authority and the Delegee

9.1 The communication between the relevant government or public authority and the delegee should include the following provisions, a copy or summary of which should be forwarded to ICANN:

9.1.1 Term, performance clauses, opportunity for review and process for revocation.

9.1.2 A commitment by the delegee to operate the ccTLD in the interest of the relevant local community and the global Internet community.

9.1.3 A recognition by the delegee that the management and administration of the ccTLD are subject to the ultimate authority of the relevant government or public authority, and must conform with relevant domestic laws and regulations, and international law and international conventions.

9.1.4 Confirmation that the ccTLD is operated in trust in the public interest and that the delegee does not acquire property rights to the ccTLD itself.

9.1.5 Conditions to ensure the transfer of all relevant DNS data to a nominated replacement, if, for any reason, a reassignment to a new delegee is necessary.

9.1.6 Conditions for the efficient and effective resolution of disputes arising from domain name registration. In so far as ccTLD registration policies allow or encourage registrations from entities or individuals resident outside the relevant territory, then the delegee concerned should implement dispute resolution policies that ensure that the interests of all registrants, and of third parties, including those outside their territory and in other jurisdictions, are taken into account. Dispute resolution policies should, to the greatest extent possible, follow common

principles, including due regard for internationally recognised intellectual property, consumer protection and other relevant law, and be implemented by all delegees. The delegee should, so far as possible, implement alternative dispute resolution procedures conducted online, without precluding access to court litigation.

9.1.7 The delegee's commitment to abide by ICANN developed policies as set forth in Clause 10.

9.1.8 Where ccTLD registration policies allow or encourage registrations from entities or individuals resident outside the relevant territory, the delegee commits to observe all ICANN policies applicable to such ccTLDs, not otherwise provided for in Clause 10, except where the delegee is prohibited by law from, or instructed in writing by the relevant government or public authority to refrain from, implementing such other ICANN policies.

9.1.9 The above terms and conditions shall apply to delegees, including delegees who are resident and/or incorporated outside the territory of the relevant local community.

9.2 A delegee should not sub-contract part or all of the technical operations of the ccTLD registry without ensuring that the sub-contractor has the technical qualifications required by ICANN, and informing ICANN.

9.3 In any sub-contracting of the technical operations of the ccTLD registry or administrative and management functions of the ccTLD, the sub-contract must state that the delegation itself is an exercise of a public right, not an item of property, and cannot be reassigned to a new delegee except in accordance with the provisions of Clause 7.

10. Principles concerning the Communication between ICANN and the Delegee

10.1 The communication between ICANN and the delegee should contain ICANN's commitment to:

10.1.1 maintain, or cause to be maintained, a stable, secure, authoritative and publicly available database of relevant information for each ccTLD (see below);

10.1.2 ensure that authoritative and accurate root zone information is generated from such database and ensure that the root servers are operated in stable and secure manner;

10.1.3 maintain, or cause to be maintained, authoritative records and an audit trail regarding ccTLD delegations and records related to these delegations; and

10.1.4 inform the delegee in a timely manner of any changes to ICANN's contact information.

10.2 The communication between ICANN and the delegee should contain the delegee's commitment to:

10.2.1 cause to be operated and maintained in a stable and secure manner the authoritative primary and secondary nameservers for the ccTLD, adequate to resolve names within the ccTLD for users throughout the Internet, and any sub-domains over which they retain administrative authority, and ensure that the zone file and accurate and up-to-date registration data is continuously available to ICANN for purposes of verifying and ensuring the operational stability of the ccTLD only;

10.2.2 inform ICANN in a timely manner of any changes to the ccTLD's contact information held by ICANN;

10.2.3 ensure the safety and integrity of the registry database, including the establishment of a data escrow or mirror site policy for the registry data managed by the delegate. The escrow agent or mirror site should be mutually approved by the relevant government or public authority and the delegee and should not be under the control of the delegee;

10.2.4 ensure the transfer of all relevant DNS data to a nominated replacement, if, for any reason, a reassignment to a new delegee is necessary;

10.2.5 abide by ICANN developed policies concerning: interoperability of the ccTLD with other parts of the DNS and Internet; operational capabilities and performance of the ccTLD operator; and the obtaining and maintenance of, and public access to, accurate and up-to-date contact information for domain name registrants; and

10.2.6 ensure the payment of its contribution to ICANN's cost of operation in accordance with an equitable scale, based on ICANN's total funding requirements (including reserves), developed by ICANN on the basis of consensus.

Bilagan har i sin helhet hämtats från Domännamnsutredningens betänkande ".se?", SOU 2000:30.

Domännamnssystemet – en snabbintroduktion

Lars-Johan Liman
Kungliga Tekniska Högskolan
Version 2.0, 1999–09–20

Innehåll

1 Problemet

Det lättaste sättet att föreställa sig problemet är att tänka sig att man har beställt en telefon och just fått den installerad. Man sitter där med sin fina apparat och man kan i princip ringa till hela världen. Man kan namn och adress på en massa människor man vill prata med, problemet är att man inte kan några telefonnummer. Man behöver en telefonkatalog eller en nummerbyrå.

På Internet fungerar det på samma sätt. Internet är helt världsomspännande, och lokala telefonkataloger anses utan värde. Det behövs en global telefonkatalog som täcker hela systemet. Av samma anledning som man inte har hela världens telefonkatalog i sin bokhylla – den blir alldeles för stor, och den blir alldeles för snabbt inaktuell – så har datorerna på Internet inte heller någon sammanhållen, central katalog; de har faktiskt ingen katalog alls. Man har satsat helt och hållet på en snabb och väl fungerande nummerbyrå: domännamnssystemet (DNS). Systemet är distribuerat på ett hierarkiskt sätt, så att den som är ansvarig själv kan sköta sin del av databasen. Med hjälp av snabba hänvisningar kan den som letar snabbt hitta fram till rätt databasserver.

2 Historik

Så länge datorer har funnits har människan givit dem namn. Redan de allra första datorerna döptes. BARK och BESK blev snabbt rikskändisar. När man kopplar ihop datorerna i nätverk blir det viktigt att veta vilken dator man kommunicerar med. En dators identitet på ett nätverk är i allmänhet ett tal (datorer arbetar ju bara med tal), och datorerna sinsemellan har inga problem att hålla isär varandra med hjälp av tal, men vi människor har det.

Internet är inget undantag. Alla datorer på Internet identifieras med sitt eget tal – sitt ”telefonnummer” om man vill. Denna *Internetadress* är svår för människor att komma ihåg (talen är stora, från 0 upp till 4294967295), och kan också ändras med tiden. Oftast skrivs adresserna som fyra grupper av mindre tal (t.ex. 192.168.11.1) för att de skall bli lättare att minnas och att hantera, men det är bara ett annat skrivsätt.

Människor som arbetar med datorer vill kunna säga åt sina system ”Koppla dig till den där andra datorn!”. På något sätt måste man identifiera ”den andra datorn”. Man skulle kunna använda

talen: ”Koppla dig till datorn som har adress 10244753!” ... eller var det 10244735 ... eller 10244357? Rent tekniskt fungerar det, men människans hjärna är dålig på att komma ihåg långa sifferserier. Man vill mycket hellre säga åt sitt system ”Koppla dig till datorn som heter besk!”. Datorn kan tolka namnet besk och på något sätt slå upp vilken adress just besk har, och sedan koppla sig till den adressen. Bara den människa som en gång ställer i ordning systemen behöver bekymra sig om vilken faktisk adress som besk har, men så snart det är inskrivet i uppslagstabellen så kan man sluta bry sig. Det går ju att slå upp i sagda tabell.

På Internet förde man länge en central sådan tabell som innehöll namn på alla datorer på Internet och vilken adress de hade. Tabellen distribuerades till samtliga maskiner som var anslutna till det då för tiden tämligen hanterliga lilla nätet, så att maskinerna kunde hålla reda på vad alla andra hette och vilka adresser de hade. Tabellen blev längre... och längre... och längre. Varje dator måste dessutom ha ett unikt namn för att det inte skulle bli några krockar. Fantasin tröt. När tabellen hade blivit ett antal tusen rader lång, och en ansenlig andel av nätets kapacitet gick åt till att skicka denna tabell kors och tvärs mellan alla datorer, insåg man varthän det var på väg och uppfann ett nytt system – domännamnssystemet (DNS).

DNS innebar två radikala skillnader:

1. *Hierarkisk namngivning*. För att ge flera datorer möjlighet att ha samma namn, införde man längre namn med flera namndelar. I början grundade sig namndelarna på vilken typ av organisation man tillhörde, och vad organisationen hette. Ganska snart infördes landskoderna, och någon i respektive land fick ansvaret för tilldelningen av namn inom det landet.
2. *Dynamisk uppslagning*. Man skrotade den gemensamma tabellen, och skapade ett system med databasservrar som hänvisar till varandra enligt samma hierarkiska system som namnen följer. Ingen dator har alltså mer information än vad den själv ansvarar för och vad som behövs för att knyta ihop den med övriga servrar i brödraskapet. Genom att fråga sig fram kan man nu hitta den information man söker.

3 Definitioner

Eftersom följande text kommer att handla en del om databaser och hantering av dem, är det viktigt att först klargöra några begrepp.

3.1 Uppslagsnyckel – värde

En uppslagsnyckel är en textsträng eller ett tal som man använder för att hitta fram till andra data. Om man vill veta Pelles telefonnummer och skall titta i sin lilla telefonbok så slår man på ”P” som i Pelle och där står det antagligen

Pelle	01 – 17 47 11

”Pelle” är strängen man använder för att hitta fram till rätt telefonnummer, och den kallas uppslagsnyckel.

Den information man ville åt var ju själva telefonnumret: 01 - 17 47 11. Denna information kallas ”värdet”. *Nyckeln* är alltså den information som man har, och som man använder för att hitta annan information. *Värdet* är den information man letar efter.

3.2 Post

En post är just en kombination av en nyckel och ett värde. Ofta innehåller posten mer information, t.ex. vad det är för typ av värde. En post kan också innehålla flera olika värden av samma eller olika typ, t.ex.

Pelle	Tel 01 – 17 47 11
Telefon:	0701 – 47 33 00
Adress:	Minnesstigen 23; 100 99 DATABO
E-post:	pelle@acme.se

Denna post har uppslagsnyckeln ”Pelle”. För att sedan hitta precis den information man vill ha måste man bestämma sig lite noggrannare – är man ute efter telefonnumret eller adressen? I databassammanhang kallar man ofta de olika delarna i en post för *fält*.

I DNS-sammanhang har man i stället flera poster med samma uppslagsnyckel, och sedan olika typer av poster beroende på vilken

typ av information som finns lagrad i dem. Om detta system tillämpades i telefonboken ovan skulle det se ut som

Nyckel	*Posttyp*	*Värde*
Pelle	telefon	01 – 17 47 11
Pelle	adress	Minnesstigen 23 100 99 DATABO
Pelle	telefon	0701 – 47 33 00
Pelle	e-post	pelle@acme.se

När man vill ha tag i information använder man alltså både söknyckel och posttyp för att hitta rätt.

3.3 Uppslagning – sökning

Skillnaden mellan uppslagning och sökning är viktig. Vid en *uppslagning* har man en klar och tydlig söknyckel och förväntar sig ett (eller möjligen flera) klara tydliga värden. Man har t.ex. ett namn och vill ha tag i den personens telefonnummer. Man slår upp det och förväntar sig *ett* svar, möjligen några få om personen har fler än ett telefonnummer.

Vid en *sökning* har man en icke entydig söknyckel och man förväntar sig ett urval som svar. Ur detta urval väljer man sedan en söknyckel med vars hjälp man gör en uppslagning. Ett exempel:

> – Han hette något på P och jag behöver hans telefonnummer!
> – Här är en lista på alla som börjar på P. Vem av dem menar du?
>
> Per-Arne
> Pelle
> Petter
>
> – Jag menar Pelle. Ge mig Pelles telefonnummer!
> – Han har två: 01 – 17 47 11 och 0701 – 47 33 00.

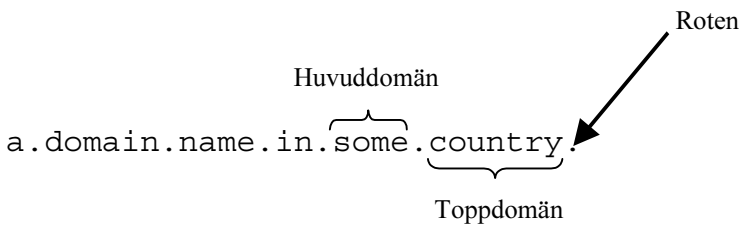
I detta exempel är söknyckeln först inte väl definierad. Den är ”något som börjar på P”. En sökning leder till en lista på alternativa nycklar – ett urval av alla nycklar som finns i databasen. Från den listan kan man sedan välja den nyckel man tycker passar bäst – Pelle i detta fall. Med hjälp av denna specifika nyckel kan man nu göra en uppslagning och få reda på det eftersökta värdet.

DNS-systemet kan inte på något sätt hantera sökningar – det kan *endast* utföra uppslagningar. Man måste alltså alltid ha fullt klart för sig *exakt* vilket namn det är man vill slå upp i DNS-systemet.

4 Domännamn

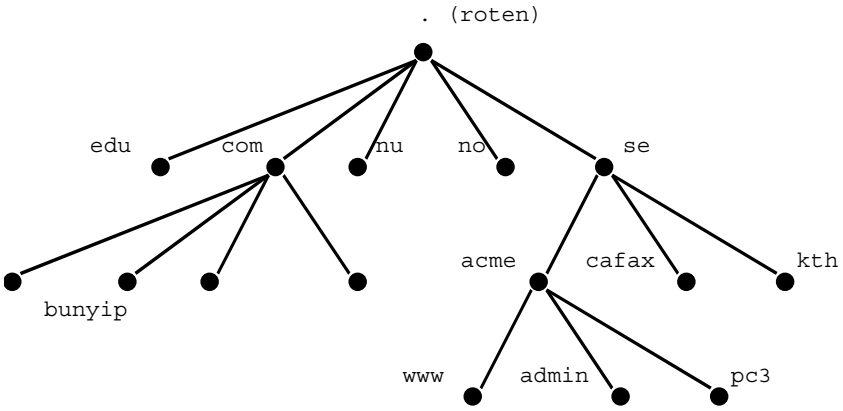
Tekniskt sett ser ett domännamn ut så här:

Ett domännamn är sammansatt av noll eller fler domändelar. Varje domändel består av en kombination av bokstäver (dock endast A–Z), siffror och tecknet bindestreck. En domändel får inte börja med bindestreck. Stor och liten bokstav tolkas lika. Domändelarna fogas samman till en sammanhängande sträng, och de olika domändelarna separeras med hjälp av tecknet punkt. Den domändel som står längs till höger kallas toppdomän (top level domain, TLD), och domändelen direkt till vänster om toppdomänen kallas ofta för huvuddomän. Ett exempel:



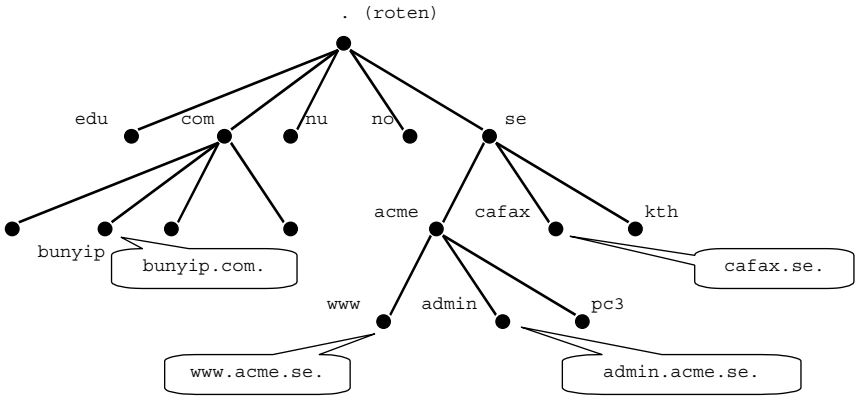
Längden på ett domännamn begränsas av följande värden: Hela namnet, inklusive alla punkter, får maximalt vara 255 tecken, samt, varje domändel måste ha minst ett tecken och maximalt 63 tecken (punkten oräknad). Med hjälp av lite matematik kommer man fram till att man alltså kan ha maximalt 126 ”nivåer” i ett domännamn. Dessa längdgränser är sällan eller aldrig något praktiskt hinder.

Domännamnen följer en strikt hierarki som bildar ett matematiskt träd, och det utgår från ett centralt namn – roten.



Figur 1: Domännamnsträdet.

När man tolkar ett domännamnsträd läser man namnen nedifrån och upp. I trädet ovan kan vi alltså utläsa namn som `bunyip.com.`, `www.acme.se.`, `admin.acme.se.`, `cafax.se.`, `se.`, osv.



Figur 2: Några domännamn.

Domännamnen lagras som uppslagsnycklar i databasen, och man kopplar olika typer av information, dvs. olika värden, till uppslagsnycklarna. Datorer på Internet kan sedan slå upp information i

databasen och använda den. Det vanligaste man lagrar i DNS-databasen är Internetadresser. En dators identitet på Internet är egentligen dess adress (numret). Genom att lagra ett domännamn i databasen och koppla en Internetadress som värde till den uppslagsnyckeln, så ger man datorn ett namn. Man kan slå upp namnet i databasen och få reda på dess adress, och därmed nå fram till den datorn. Alla webbservrar finns lagrade i DNS, och när man skriver in en URL i sitt webbverktyg (t.ex. Netscape) så används en del av URL:en som uppslagsnyckel i DNS för att man skall få fram webbserverns adress på Internet.

Man kan lagra annan typ av information i DNS-databasen också. DNS-systemet används t.ex. för att hålla reda på vilken dator som är e-postserver för en viss domän. Vill man skriva brev till `postmaster@acme.se` så slår man upp `acme.se.` i DNS och frågar efter tillhörande e-postserver. Man får då namnet på en dator som svar, och kan sedan på vanligt sätt slå upp den datorns adress genom en andra slagning i databasen. Sedan är det bara att koppla upp sig mot den adressen och skicka brevet.

Det är viktigt att inse att alla domännamn fungerar på *precis* samma sätt, principiellt sett. Det är människan som väljer hur namnen skall användas genom att koppla ihop olika typer av information med olika namn i DNS-databasen. Det är alltså ingenting som hindrar att en webbserver heter `pc3.acme.se.` eller att en vanlig PC har namnet (endast) `se.` eller att en mailadress ser ut som

```
postmaster@www.acme.se
```

4.1 Namnservrar

Domännamnen matas in i filer i DNS-servrar som är anslutna till Internet. I servrarna körs programvara som läser in filerna och sedan lyssnar efter DNS-frågor från nätverket och gör sitt bästa för att svara på dem.

En sådan databasfil kan innehålla poster som ser ut som:

```
www.acme.se.      A     192.168.3.31
pc3.acme.se.      A     192.168.4.11
acme.se.    MX    0     mailgw1.super-ip.net.
```

Ur datan ovan kan man utläsa att den som har skrivit filen vill tala om för omvärlden att det finns en dator som heter `www.acme.se.` med adressen 192.168.3.31 (A = Address), att det finns en annan dator som heter pc3.acme.se. och som har adressen 192.168.4.11, samt att man kan skicka e-post till adresser som slutar på `@acme.se.` till den dator som heter `mailgw1.super-ip.net.` så kommer den datorn att se till att e-posten kommer dit den skall (MX = Mail eXchanger).

Om det nu kommer frågor till DNS-servern ovan så kommer den att svara med det den vet. Om någon frågar ”Vad har datorn `pc3.acme.se.` för adress?”, så kommer den att svara ”192.168.4.11”.

4.2 Rotnamnservrar och hänvisningar

I teorin skulle man kunna lagra alla domännamn i en och samma server. Ingenting i systemdesignen förhindrar att man gör det, men det blir inte praktiskt. Om vi går tillbaka till jämförelsen med nummerbyrån, så skulle man kunna ha en nummerbyrå för hela världen. Det fungerar inte rent praktiskt eftersom det skulle behövas oändligt många telefonister, oändligt stora kataloger för dem, en gigantisk ström av uppdateringar från alla i hela världen som flyttar eller byter nummer, samt att det innebär att hela världen blir beroende av en enda informationspunkt för att kunna ringa.

I DNS-världen har man samma problem. Det går inte att ha all information i en och samma server av praktiska skäl. Man har i stället delat upp informationen så att olika servrar har hand om olika delar av den. Vid varje punkt i ett domännamn *kan* man införa en teknisk ansvarsgräns. Två saker är viktiga här: för det första är det fråga om att man *kan* ha en gräns vid varje punkt, men man måste inte; för det andra är det fråga om *tekniska* gränser, dvs. gränser och signalering mellan servrar, inte om vilken organisation eller administration som har ansvar för namnen i sig.

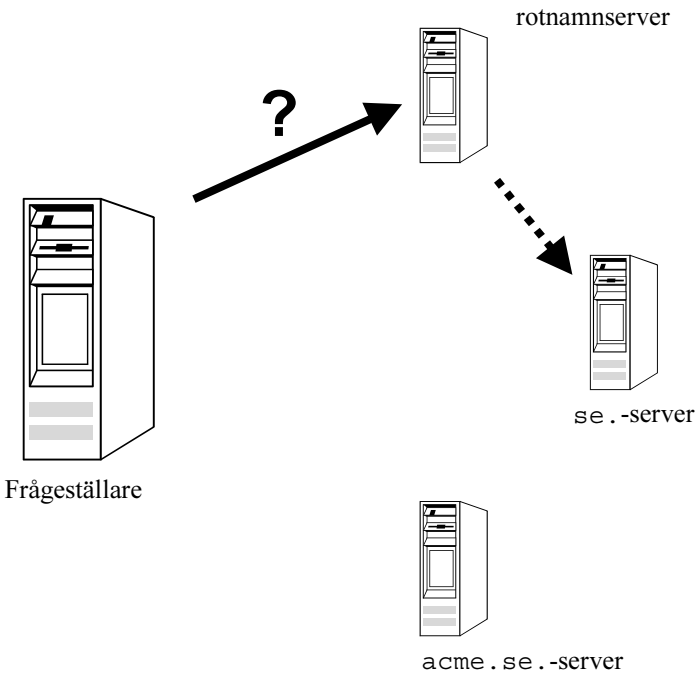
Mellan servrarna som har hand om olika informationsmängder finns sedan ett system av hänvisningar. Genom att fråga sig fram och med hjälp av hänvisningarna kan man alltid hitta fram till den server som har hand om en viss del av informationen. Hänvisnings-systemet skulle kunna bli väldigt komplext om alla skall kunna

hänvisa till alla andra, men för att undvika det problemet så följer hänvisningarna domännamnsträdet helt slaviskt.

Tjuvknepet i DNS-världen är att man inte i förväg talar om för någon att det finns hänvisningar i systemet. Alla datorer tror att det bara finns en nummertjänst. Det finns en namnserver som har hand om roten till DNS-systemet. Den innehåller bara en liten, liten databas (mindre än 1/10 av en vanlig PC-diskett). I den databasen finns bara hänvisningar. Om man frågar denna rotnamnserver någon DNS-fråga så kommer man alltid bara att få till svar ”Jag vet inte, prata med honom därborta!”, men det är just det som är det viktiga, rotnamnservern håller reda på vem man skall prata med. Hänvisningarna kan finnas i alla nivåer i databasen, och rotnamnservern är bara den första man frågar. Man kan bli hänvisad flera gånger, men börjar man med rotnamnservern så kan man alltid komma fram dit man skall.

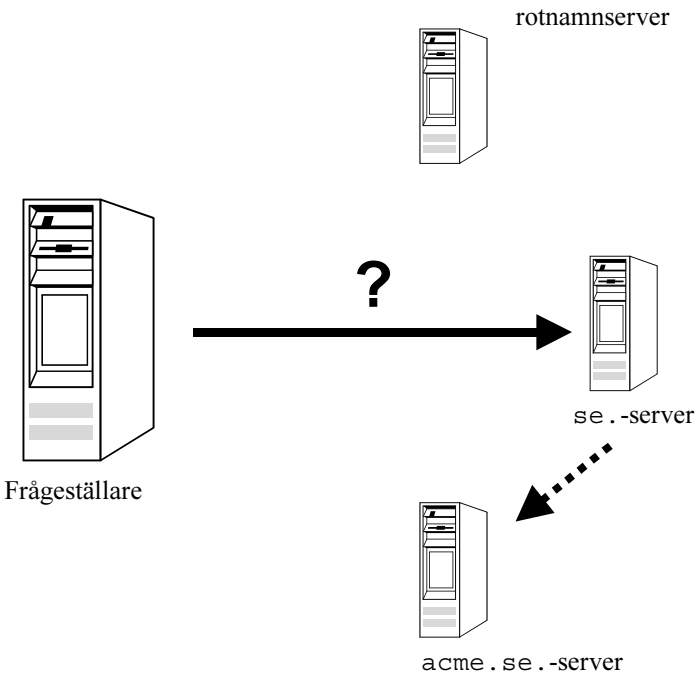
4.3 Uppslagning: ett exempel

Låt säga att vi vill veta vad webbservern `www.acme.se.` har för Internetadress. Det vi skall slå upp i DNS-databasen är alltså adressposten för namnet `www.acme.se`. Vi frågar alltså rotnamnservern vad `www.acme.se.` har för adress.



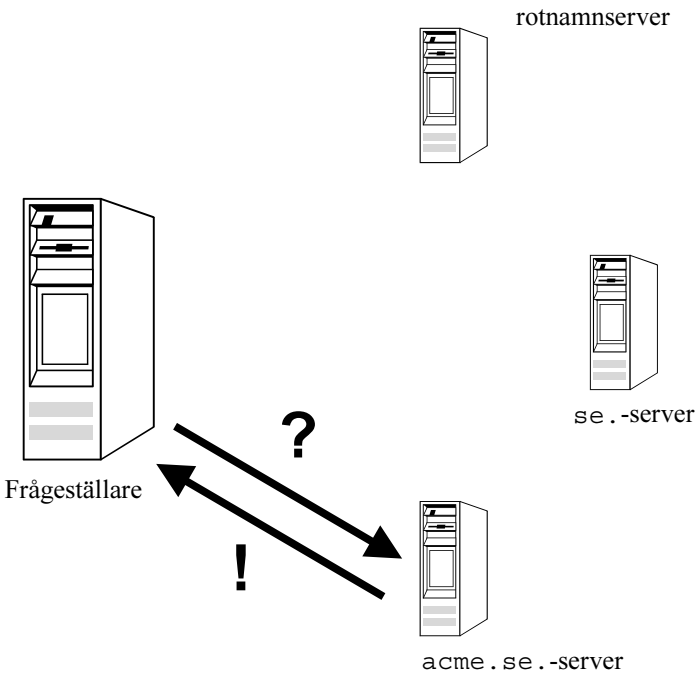
Figur 3: En fråga, steg 1: rotnamnservern och hänvisning.

Rotnamnservern svarar på sitt vanliga manér: ”Jag vet inte, men jag ser att det du frågar om slutar på `se.`, och då skall du prata med den där datorn där borta, för det är den som har hand om allt som slutar på `se`.”. Vi blir alltså hänvisade till en annan dator som förväntas känna till mer. Vi skickar då samma fråga till denna `se.`-server: ”Vad har `www.acme.se.` för adress?”.



Figur 4: En fråga, steg 2: `se.`-servern och vidare hänvisning.

Till svar får vi kanske ytterligare en hänvisning: ”Jag vet inte, men jag ser att det du frågar om slutar på `acme.se.` och då skall du prata med den servern därborta.”. Vi går vidare igen, och ställer nu samma fråga för tredje gången, nu till en tredje dator: ”Vad har `www.acme.se.` för adress?”.



Figur 5: En fråga, steg 3: svaret.

Sannolikt får vi nu veta svaret: ”www.acme.se. har adressen 192.168.3.31.”. Äntligen kan vi koppla upp oss mot webbservern och hämta de webbsidor vi var ute efter.

Beskrivningen ovan lämnar bl.a. följande frågor öppna:

Hönan och ägget

1. *Hur vet man var rotnamnservern finns?* För att man alltid skall kunna ringa någonstans, så är telefonnumret till nummerupplysningen publicerat och gjort allmänt känt, genom media och informationskampanjer. Folk kan det utantill, och ingen behöver tveka om vilket nummer som är rätt. Eftersom alla känner till det så går det inte att förfalska. På samma sätt måste alla datorer som vill kunna använda DNS-systemet veta vilken adress rotnamnservern har. Internetadressen till rotnamnservern är alltså

allmänt känd. Den finns publicerad på flera ställen, och tillhandahålls av operatörer och andra i branschen. Alla namnservrar har den listan liggande i en fil, och man kan lätt kopiera den mellan olika namnservrar.

Redundans

2. *Vad händer om rotnamnservern stannar eller tappar kontakten med nätverket?* Det finns inte bara en enda rotnamnserver. Det finns totalt 13 rotnamnservrar i världen och alla har identiska kopior av databasen. Om en tillfälligt försvinner väljer man bara en annan. Det finns följaktligen egentligen 13 olika adresser att hålla reda på. Programvaran som ställer frågor läser in de 13 adresserna från en fil och väljer sedan helt automatiskt vilken rotnamnserver den vill prata med och byter om det blir nödvändigt. Det är alltså inte kritiskt att alla rotnamnservrar hela tiden är tillgängliga. Internet skulle klara sig alldeles utmärkt även om hälften av dem försvann.

Vidare genom systemet

3. *Hur vet man var `se.`-servern finns?* Det ingår i själva hänvisningen som kommer från rotnamnservern. Rotnamnservern vet alltså var den finns och talar alltid om det när den hänvisar.

Redundans på alla nivåer

4. *Vad händer om `se.`-servern stannar eller tappar kontakten med nätverket?* På samma sätt som med rotnamnservern så finns det inte bara en server som håller reda på alla namn som slutar på `se.` I fallet `se.` finns det sju servrar som har identiska kopior av den delen av databasen. När en rotnamnserver hänvisar, så hänvisar den till alla sju. ”Fråga någon av de här sju datorerna, med de här sju adresserna. Alla av dem vet mer än jag.”

Master- och slavservrar

5. *Hur ser man till att kopiorna är identiska?* Servrar som skall ha identiska kopior av en viss del av databasen är konfigurerade så att en av dem är *masterserver* (kallades tidigare *primary server*). De övriga servrarna, *slavservrarna* (*secondary servers*), i gruppen kontrollerar med jämna mellanrum om masterserverns exemplar av databasen har ändrats genom att ställa en speciell fråga till den. Om en slavserver upptäcker att masterservern har en nyare version av innehållet i databasen än vad den själv har, ber den masterservern att skicka över den nya versionen av innehållet. För enkelhets skull kopieras i allmänhet hela databasdelen vid varje sådant tillfälle, inte bara ändringarna. Skall något ändras i en viss del av DNS-databasen, så ändrar man alltså i masterservern för den delen av databasen, varefter slavservrarna så småningom kopierar informationen till sig, och alla kommer att ha identiska kopior. Det blir alltså vanligen ett visst tidsglapp just vid uppdateringar, när masterservern har en nyare version av databasinnehållet än vad slavservrarna har. Eftersom man oftast bara ändrar små detaljer i databasen, så är kopiorna i alla fall ”nästan rätt” till dess att kopieringen har skett fullt ut, så det gör inte så mycket. Moderna masterservrar talar också om för sina slavar när det har skett en uppdatering, så att slavarna snabbt kan kopiera en ny version av databasdelen.

Cachening

6. *Blir det inte väldigt hög belastning på rotnamnservrarna?* Inte så hög som man skulle kunna tro. Anledningen är att inte alla frågeställare går till rotnamnservern först. En frågeställare sparar nämligen alla svar en viss tid. Om frågeställaren i exemplet ovan strax efteråt vill ha tag i adressen till `pc3.acme.se`. så kommer den ihåg att ”Jag frågade nyss rotnamnservern om ett namn som slutade på `se`. men då fick jag bara en hänvisning till svar. Jag går direkt till någon av `se`.-servrarna han hänvisade till.”. Eftersom även svar nummer två ovan sparades kan man till och med hoppa över nästa steg med samma resonemang. ”Jag frågade nyss en `se`.-server om ett namn som slutade på `acme.se`. och då fick jag bara en

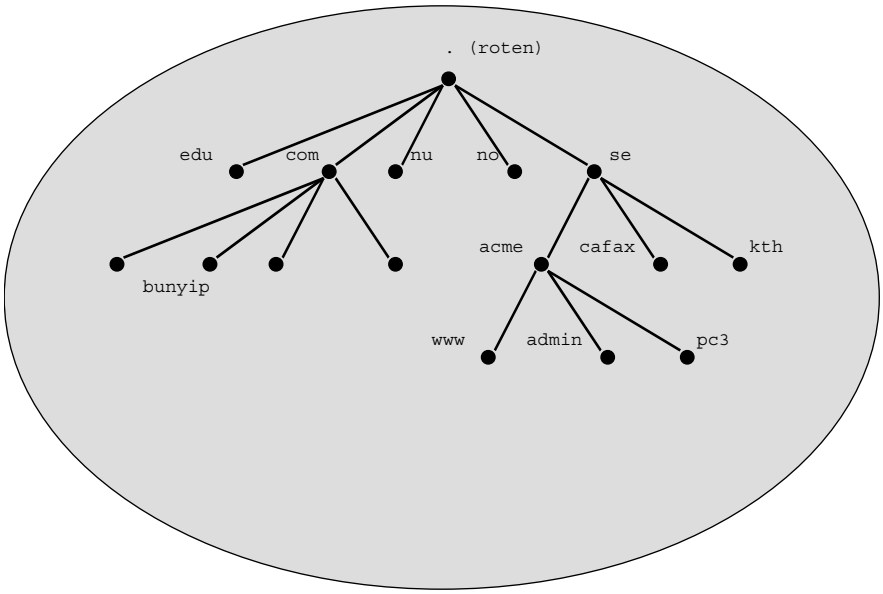
hänvisning. Jag går direkt på `acme.se.`-servern.” Varken rotnamnservern eller `se.`-servern behöver alltså bli inblandade i denna andra fråga, och belastningen på dem minskar drastiskt. Gäller frågan i stället datorn `server.cafax.se.` så kan man hoppa över steg ett, men inte steg två. Detta sätt att ”gömma undan” svaren nära till hands och återutnyttja dem kallas *cachening* (av franskans *cache* = gömställe) och är en vanlig teknik för att spara resurser i många datorsammanhang.

5 Delegeringar

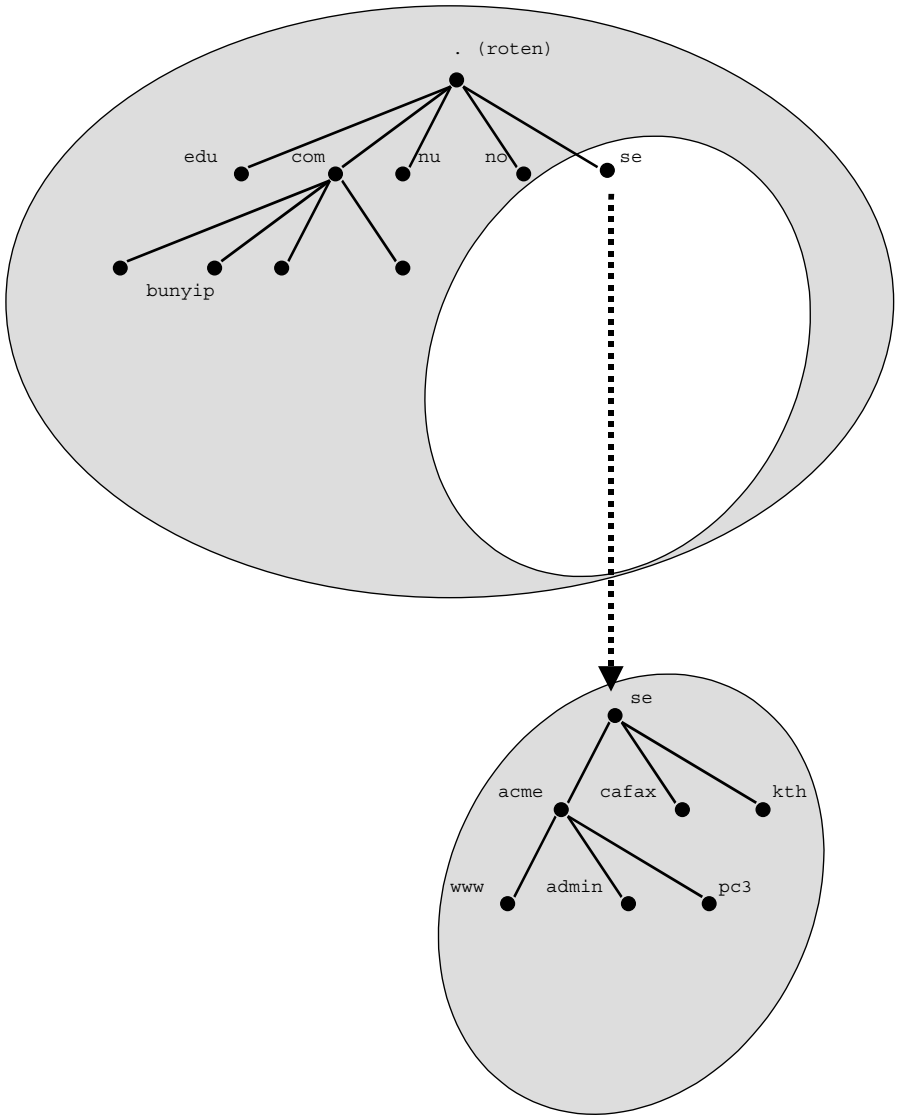
Systemet med hänvisningar och cachening är fiffigt ur flera synvinklar: dels skapar det en lokalitet i systemet som gör att den som har ansvar för själva informationen lätt kan uppdatera sin del av databasen utan att blanda in andra, dels minskar belastningen på servrarna högre upp i systemet.

Hänvisningarna kallas på DNS-språk för *delegeringar*. En DNS-databasdel innehåller enkelt uttryckt ”alla uppslagsnycklar som slutar på ett visst domännamn utom de namn man har delegerat ut”. Låt oss gå tillbaka till namnträdet.

Man kan tänka sig att när DNS-systemet startades låg allting i samma fil på samma server. Efterhand har man delat ut ansvaret för en viss domän till någon annan, och då flyttar man bort all information om den domänen ur den befintliga servern och lägger den i en ny server. I den gamla servern stoppar man in en hänvisning till den nya servern i stället för all gammal information.

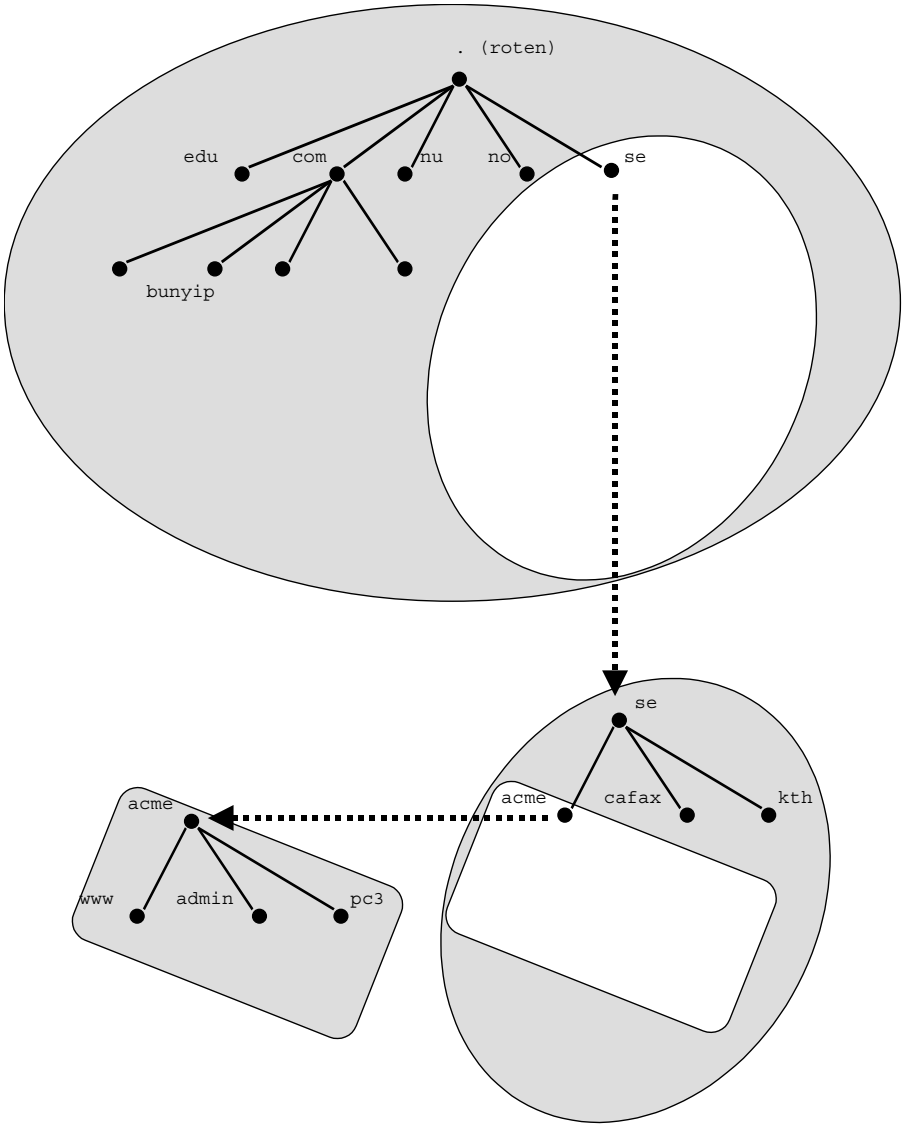


Figur 6: Före delegering av se.-domänen.



Figur 7: se.-domänen delegeras ut till en annan server.

Delegering av domäner sker på samma sätt på alla nivåer i DNS. Det är alltså fullt möjligt att ur se.-domänen i sin tur delegera ut t.ex. domänen acme.se. Det skulle se ut så här i vårt träd.



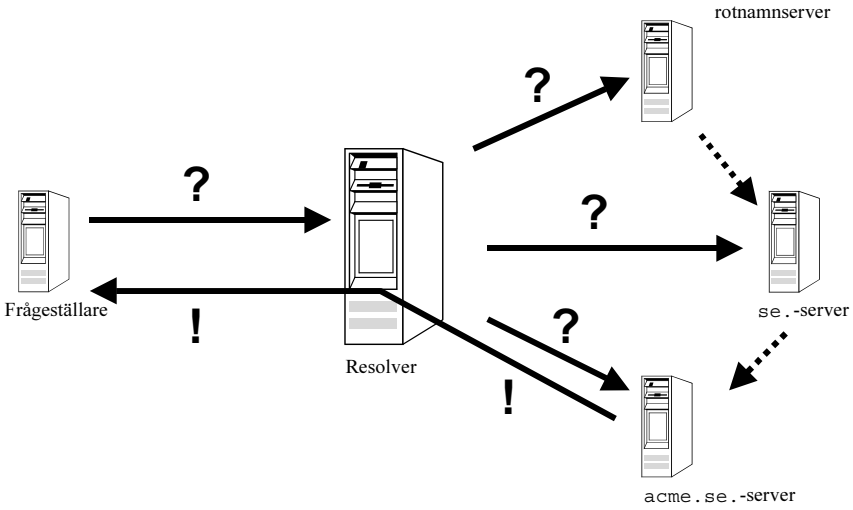
Figur 8: acme.se. delegeras ut ur se.

Vi kan se att information om `bunyip.com`. fortfarande ligger kvar hos rotnamnservern i vårt exempel, och att information om `kth.se.` ligger kvar hos den server som har hand om `se`. Följande princip gäller alltså: om man inte har delegerat ut ett domännamn, ligger det tekniska ansvaret för databasen för den domänen hos den server som har den omslutande (eller överliggande, om man vill) domänen, och den omslutande domänen *kan* finnas flera steg upp i trädet (`bunyip.com.` handhas inte av `com.` utan av roten i detta exempel).

6 Resolvers

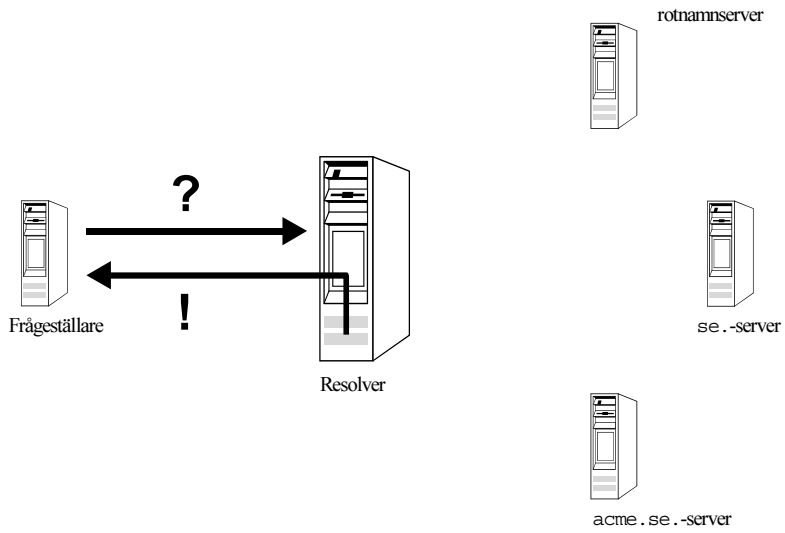
Det finns två typer av DNS-tjänster en dator kan tillhandahålla. Den kan innehålla en del av databasen och svara på frågor angående den del av databasen den innehåller, som jag har beskrivit ovan, men den kan också vara av typen tjänst till andra lokala datorer att leta upp svaret på vilken DNS-fråga som helst.

De flesta vanliga datorer har inte programvara som klarar att traversera DNS-trädet, dvs. att gå till rotnamnservern, följa hänvisningar (kanske i flera steg), cachea information osv. Det är ett omfattande arbete som kräver en hel del programkod. Att skicka en enstaka DNS-fråga är däremot inte så svårt, så det klarar alla datorer idag. För att lösa problemet finns det DNS-servrar som hjälper till att svara på frågor. Till dem kan man ställa vilken DNS-fråga som helst, varvid de så att säga ”på uppdrag” går ut och traverserar (letar igenom) DNS-trädet, följer hänvsningar, cachear och allt som skall till. När de har hittat svaret skickas det tillbaka till frågeställaren. Frågeställaren har alltså inte behövt göra något mer än att skicka en enda fråga till en viss bestämd, närbelägen server och sedan bara vänta på svaret.



Figur 9: Resolvern hjälper till att hitta DNS-information.

Resolvern cachear som sagt alla svar den får från andra servrar. Om en (annan?) frågeställare kommer strax efter och frågar efter samma information som resolvern nyss har hämtat fram, så finns ju svaret i cachen, och resolvern har då ingen anledning att upprepa manövern utan svarar med var den redan vet.



Figur 10: Resolvern svarar ur sin cache om den kan.

7 Säkerhet

DNS-systemet är troligen världens största distribuerade databas. Var och en kan sköta sin egen del av databasen. Denna lokala administration underlättar arbetet att hålla databasen uppdaterad, men eftersom det hittills inte har funnits någonting i DNS som verifierar vem som har stoppat in vilken information, så leder det också till att det är lätt att ”ljuga” – dvs. stoppa in falsk information och t.ex. utge sig för att vara någon annan än den man egentligen är. Falsk DNS-information öppnar möjligheter för att stjäla annan information (e-post och annat) och störa transaktioner (elektronisk handel, fakturor m.m.). Det är också viktigt att med säkerhet kunna veta att något *inte* existerar i DNS, så att inte frånvaron av information kan förfalskas.

Särskilt påtagliga blir problemen om man vill använda dynamisk DNS, dvs. man vill tillåta datorer på nätet att införa förändringar i DNS-informationen i körande DNS-system. Det är då extra viktigt att säkerställa att informationen kommer från rätt källa.

Problemen har naturligtvis uppmärksammats och det finns nu tekniker för betydligt säkrare hantering av DNS-information med hjälp av Secure DNS (DNSSEC).

7.1 Secure DNS

Grundconcepten i DNSSEC är checksummor och asymmetrisk kryptering. Checksummor är tal man får fram genom att applicera en slug matematisk algoritm på en viss informationsmängd. Algoritmen är så utformad att minsta ändring av informationen leder till en förändring av checksumman.

Om den ärliga DNS-servern räknar ut checksumman för alla sina poster i DNS, och sedan krypterar cheksummorna en efter en, samt bilägger den krypterade checksumman till respektive post när den svarar på DNS-frågor, så kan frågeställaren beräkna en egen checksumma för DNS-posten och jämföra den egna med den medskickade checksumman. Om checksummorna är lika kan man vara säker på att informationen inte har förvanskats på vägen, och att den verkligen kommer från rätt ”avsändare”.

7.2 Asymmetrisk kryptering

För att detta skall fungera måste frågeställaren kunna dekryptera den medskickade checksumman. Detta kan man åstadkomma med asymmetrisk kryptering. Vid asymmetrisk kryptering har man alltid två kryptonycklar som bildar ett par; en nyckel för att kryptera med, och en annan för att dekryptera med. DNS-administratören för en domän beräknar checksummor för alla sina poster, och krypterar dem med den ena nyckeln. Den nyckeln håller han mycket hemlig. Genom att publicera den *andra* nyckeln (den för dekryptering) vitt och brett, kan alla som så vill få tag i den och använda den för att dekryptera de medsända checksummorna vid DNS-trafik.

Kvar är nu ”bara” problemet att kontrollera att det är rätt dekrypteringsnyckel man har fått tag i. För att klara det problemet har DNSSEC inbyggda mekanismer för att även tillhandahålla dekrypteringsnycklarna på ett genomtänkt och säkert sätt. Dekrypteringsnycklarna lagras också som poster i DNS, och är därmed allmänt tillgängliga. Nycklarna förses med checksummor av precis

samma typ som all annan DNS-information, och man kan då även verifiera nycklarnas äkthet.

Frågeställaren måste kunna lita på roten till all information, och måste ha tillgång till en nyckel från början för att ”komma igång”. Denna nyckel kommer att vara så allmänt känd att det kommer att bli omöjligt att förfalska den.

Denna nya säkerhetsteknik för DNS är ganska komplicerad men höjer säkerheten drastiskt. Det kommer att ställas betydligt större krav på DNS-frågeställarna om de vill kunna utnyttja tekniken. Det blir många checksummor att räkna och mycket dekrypterande att göra och bägge är resurskrävande transaktioner. Samtidigt är den nya tekniken helt bakåtkompatibel vilket gör att befintliga DNS-system som inte kan eller vill utnyttja säkerhetstekniken kommer att kunna fortsätta köra precis som vanligt, utan några större förändringar i resursåtgången.

Secure DNS finns ännu inte implementerat i någon större mängd befintliga produkter på marknaden. För att det skall bli användbart måste såväl DNS-servrar som klienter skrivas om så att de utnyttjar den nya tekniken. När det gäller den vanligaste produkten på serversidan (Berkeley Internet Name Deamon, BIND) pågår ett hektiskt arbete att uppdatera koden. Senaste versionen (augusti 1999) klarar nätt och jämnt av att hantera secure DNS, men bara på experimentstadiet. Under hösten hoppas man komma med test-versioner av en ny, från grunden omdesignad server, som skall klara secure DNS fullt ut. På klientsidan är det nog värre. Säkerhetstänkandet måste slå igenom ända ut till den lokala PC:n om det skall ge full effekt, och det innebär att man måste ändra i TCP/IP-stacken på Windows och i OpenTransport på Macintoshar samt motsvarande i andra system. Sådana ändringar kan visserligen införas med samma tidsaspekt (något år), men det finns en enorm installerad bas, och innan den är uppgraderad har det nog gått flera år.

7.3 Secure DNS i Sverige

Hur långt har man då kommit i Sverige med införandet av DNS? Ganska långt. På tekniksidan kan nämnas att svenska DNS-tekniker deltar i internationella arbetsgrupper för standardisering av Internetprotokoll. Man har internationellt också börjat experimentera med de testimplementationer som finns, och även där

deltar svenska aktörer. Den svenska domännamnsregistraturen utvecklar tekniska system för hantering av signaturer och annat.

Den administrativa sidan kräver mer eftertanke. När man arbetar med säkring av system är det viktigt att den information man baserar sin tekniska säkerhet på är korrekt. Om man t.ex. utför en DNS-delegering och signerar den, så gäller det att man verkligen vet att det är rätt person/organisation man delegerar DNS-domänen till. Man måste alltså bygga upp en organisation för att säkert identifiera den som ansöker om ett domännamn. Den svenska domännamnsregistraturen har uppmärksammat problemen och arbetar på att skapa en lösning där arbetsbelastning och säkerhet balanserar varandra på ett rimligt sätt.

All säkerhet på Internet bygger på kryptering och förhoppningen om att det är svårt och omständligt att forcera krypton. För att detta skall vara sant krävs det att man använder kryptometoder som faktiskt motsvarar den förhoppningen. Ju starkare datorer ”motståndaren” har, desto starkare kryptosystem måste man använda för att skydda sin information rimligt lång tid. Med de datorer som var och en har på skrivbordet i dag kan man ganska enkelt forcera vanliga kryptosystem. För att skydda sin information, t.ex. DNS-informationen, måste man alltså använda starka kryptosystem. Starka kryptosystem är en absolut förutsättning för någon som helst säkerhet på Internet.

Hur vet man då om en kryptometod är stark? Det finns bara ett sätt: att låta många experter undersöka metoden och förhoppningsvis bli överens om att den håller vissa mått. Det går inte om metoden är hemlig. En hemlig kryptometod är alltså en dålig bas för säkerhet, för vem vet om den är så bra som myndigheten eller företaget påstår? Varför är den hemlig? Styrkan hos en bra kryptometod är inte beroende av om andra människor känner till metoden eller inte, utan bara av att andra människor inte känner till kryptonycklarna man använt.

”Smarta kort” är en ”lösning” som lanseras då och då. Smarta kort kan man ha till mycket, bl.a. till att lagra kryptometoder och kryptonycklar av olika slag, men de har också flera nackdelar. I *vissa* av förslagen är metoderna hemliga, vilket, som framförts ovan, inte är en lämplig lösning. En annan vanlig nackdel är att kryptonyckeln i kortet stoppas dit av någon man inte känner. En direkt följd blir att denna andra människa/organisation alltså har tillgång till nyckeln, och därvid kan kopiera den, och alltså senare använda den. Det kan vara fråga om att någon anställd på bolaget

som tillverkar korten uppträder oegentligt, eller att någon av statens myndigheter systematiskt samlar in alla medborgares nycklar för att kunna använda dem i olika former av myndighetsutövning. Det gäller här att starkt värna om privatpersoners och företags integritet. Problemet kan undvikas genom att personer själva skapar sina nycklar, och sedan lämnar dem krypterade till kortföretaget, så att ingen annan kan läsa dem. Det kan dock bli administrativt komplicerat. Man måste också vara väldigt försiktig med datorer som läser korten, och skapa system som gör det svårt för sådana datorer (t.ex. snabbköpskassor) att spara informationen och utnyttja den igen, på sätt som liknar de falska bankomater som lagrade kortnummer och kod.

Ytterligare en nackdel, som hemliga metoder och smarta kort har gemensam, är bristen på standardisering. Man kan säkert införa en nationell standard för att använda en viss metod eller en viss typ av smart kort, men Internet är en internationell företeelse, och om man vill att handel och informationsutbyte skall kunna fungera mellan Sverige och andra länder, krävs det att de säkerhetsmetoder man använder har internationellt stöd.

Hur får man tag i kryptoprogramvara? Det lättaste sättet för de flesta Internetanvändare att installera ny programvara, är att hämta den från Internet. Om man vill få stor spridning på användandet av Secure DNS, krävs det att sådan programvara är lätt tillgänglig för alla, och import och export måste kunna ske obehindrat. Det är viktigt att svenskar kan utnyttja teknologi från andra länder, och det är viktigt att svensk teknologi kan exporteras till andra länder om Sverige skall kunna vara en fullvärdig deltagare i ett säkert och internationellt Internet. Programvara som läggs upp lätt åtkomlig på Internet blir tillgänglig för alla, inte bara för svenskar, och eftersom det inte finns någon metod att identifiera vem som är ”svensk” på Internet, måste export av kryptoprodukter tillåtas om produkterna skall kunna vara lätt tillgängliga för svenskar. Detta torde också öka förtroendet för Sverige som en ansvarstagande nation i säkerhetsfrågor, och skulle kunna öppna en marknad för svenska företag som vill profilera sig inom säkerhetsprodukter, ett område där det finns kunnande och erfarenhet i Sverige, och det skulle kunna fungera som draghjälp åt hela IT-industrin.

Det skulle vara till stor hjälp om svenska myndigheter i sitt internationella arbete verkade för en öppenhet i dessa frågor mellan olika länder, inte bara i Västeuropa, utan också i Amerika och i andra delar av världen. Svenska myndigheter skulle också kunna

bidra till en spridning av Secure DNS genom att tidigt själva börja använda det, och därigenom skapa förtroende för metoderna. Att kunna vara säker på att man verkligen kommunicerar med rätt myndighet i den allt större elektroniska korrespondensen skulle vara en draghjälp åt hela systemet, och få upp intresset hos företag och privatpersoner.

För att Secure DNS skall kunna införas i Sverige, måste det alltså från myndigheterna sida skapas en miljö där landet har fri import, export och användning av stark kryptering, och de bör förespråka lösningar som bygger på öppna kryptometoder och på programvara och hårdvara som är öppna för fri konkurrens. Uppmuntran till internationellt samarbete och aktiv egen användning av Secure DNS från myndigheternas sida skulle snabba upp processen att sprida systemet allmänt.

8 Andra nyheter

Det händer ganska mycket på området DNS-teknik. Man har t.ex. utvecklat metoder för att bara överföra förändringar från master- till slavserver när något har uppdaterats, i stället för att, som nu, kopiera hela databasdelen. Det utvecklas också hela tiden nya typer av poster man kan lagra i DNS, såsom vilka personer som är ansvariga för olika delar av informationen, och geografisk information, samt kryptonycklar och certifikat. Även poster för den nya versionen av Internetprotokoll (IPv6) kräver nya poster för att man skall kunna använda den ordentligt.

9 Referenser

Följande referenser kan nämnas för den som vill fördjupa sig i ämnet. Den första är en bok som är mycket heltäckande och varmt rekommenderas. RFC:erna (Requests for Comments) är dokument ur den serie av dokument som reglerar tekniken på Internet. Flera RFC:er har statusen *Internet Standard*, bl.a. [2] och [3].

[1] Paul Albitz & Cricket Liu, *DNS and BIND*, 3rd Edition, O'Reilly & Associates, Inc. ISBN 1-56592-512-2.
URL: http://www.oreilly.com/catalog/dns3/

[2] P.V. Mockapetris, RFC 1034 *Domain names – concepts and facilities.*
URL: ftp://ftp.nordu.net/rfc/rfc1034.txt
[3] P.V. Mockapetris, RFC 1035 *Domain names – implementation and specification.*
URL: ftp://ftp.nordu.net/rfc/rfc1034.txt
[4] Eastlake, RFC 2535 *Domain Name System Security Extensions.*
URL: ftp://ftp.nordu.net/rfc/rfc2535.txt

Litteraturförteckning

Litteratur

Danelius, Hans, Mänskliga rättigheter i europeisk praxis, En kommentar till Europakonventionen om de mänskliga rättigheterna, 2:a uppl., 2002.

Hemström, Carl, Stiftelsernas rättsliga ställning – Enligt 1994 års stiftelselag, Stockholm, 1996.

Holmqvist, Lars, Varumärkens särskiljningsförmåga, Stockholm, Norstedts juridik, 1999

Isoz, Henning, Stiftelselagen – En kommentar, Stockholm, Norstedts juridik, 1997.

Levin, Marianne, m.fl., Praktisk varumärkesrätt, Stockholm, Norstedts juridik, 1998.

Nergelius, Joakim, Konstitutionellt rättighetsskydd: svensk rätt i ett komparativt perspektiv, Stockholm, Norstedts juridik, 1996.

Olsson, Agne Henry, Upphovsrättslagstiftningen – En kommentar, Stockholm, Norstedts juridik, 1996.

Petrén, Gustaf/Ragnemalm, Hans, Sveriges grundlagar, 12:e uppl., Stockholm, Liber, 1980.

Ragnemalm, Hans, Överlämnande av förvaltningsuppgift till enskilt subjekt, Förvaltningsrättslig tidsskrift 1976 s. 105 – 145.

Strömberg, Håkan, Allmän förvaltningsrätt, 21:a uppl., Lund, Liber, 2002.

Strömberg, Håkan, Normgivningsmakten enligt 1974 års regeringsform, 3. uppl., Lund, Juristförlaget, 1999.

Tuula, Marie, IT-bolagen och de immateriella tillgångarna: vid företagsrekonstruktion och konkurs, Stockholm, Norstedts juridik, 2002.

Ullenhag, Erik, Kärnkraftsavvecklingen och Europakonventionen, SvJT 1998, s. 315 – 340.

Rapporter

Post- och telestyrelsen, Förändringar av organisatorisk och rättslig karaktär som är nödvändiga för att Post- och telestyrelsen skall kunna verifiera eller vidta åtgärder för att säkerställa att Internet i Sverige kan drivas oberoende av funktioner utomlands, 01-023882, oktober 2001.

Post- och telestyrelsen, Internets robusthet, 01-026614, december 2001.

Post- och telestyrelsen, Drift av Internet oberoende av funktioner utomlands, 01-026615, december 2001.

Post- och telestyrelsen, Är Internet i Sverige robust? (PTS-ER 2003:1).

Informationstekniska standardiseringen, Rapport ITS 6 – Terminologi för Informationssäkerhet (numera SIS), mars 1994.

IT-kommissionen, Vem använder Internet och till vad? Spridning av Internet bland befolkningen, 1/2002.

Offentligt tryck

prop. 1971:30	Med förslag till lag om allmänna förvaltningsdomstolar, m.m.
prop. 1973:90	Med förslag till ny regeringsform och ny riksdagsordning
prop. 1975/76:209	Fri- och rättigheter i grundlag
prop. 1985/86:80	Om ny förvaltningslag
prop. 1990/91:60	Offentlighet, integritet och ADB
prop. 1993/94:9	Stiftelser
prop. 1993/94:117	Inkorporering av Europakonventionen och andra fri- och rättighetsfrågor
prop. 1995/96:125	Åtgärder för att bredda och utveckla användningen av informationsteknik
prop. 1996/97:111	Rättsligt skydd för databaser, m.m.
prop. 1997/98:44	Personuppgiftslag
prop. 1999/2000:86	Ett informationssamhälle för alla
prop. 2001/02:158	Samhällets säkerhet och beredskap
prop. 2002/03:110	Lag om elektronisk kommunikation, m.m.
SOU 1985:51	Upphovsrätt och datorteknik
SOU 2000:30	.se?

SOU 2001:41 Säkerhet i en ny tid
SOU 2002:14 Statlig tillsyn. Granskning på medborgarnas uppdrag
SOU 2002:60 Lag om elektronisk kommunikation
SOU 2002:109 Myndighetsfrågor m.m.

Rättsfall

Europadomstolen

Van Marle m.fl. mot Nederländerna, dom 1986-06-26, Ser. A Vol. 101.
Tre Traktörer Aktiebolag mot Sverige, dom 1989-07-07, Ser. A Vol. 159.
Fredin mot Sverige, dom 1991-02-18, Ser. A Vol. 192.
James m.fl. mot Storbritannien, dom 1986-02-21, Ser. A Vol. 98-B.
Pressos Compania Naviera S.A. m.fl. mot Belgien, dom 1995-11-20, Ser. A Vol. 332.

Högsta domstolen

NJA 1948 s 414
NJA 1995 s 256

Regeringsrätten

RÅ 1980 1:82
RÅ 2001 ref 72.