Nasjonal kommunikasjons-myndighet

Internett i Norge – Årsrapport 2022

Juni 2022

Innholdsfortegnelse

Sammendrag – Internett i Norge

«Internett i Norge – Årsrapport 2022» er første utgave av årsrapporten.

Rapportens hoveddel 1 beskriver tilstanden til nettnøytralitet i Norge. Nettnøytralitet er prinsippet om at internettrafikk skal behandles likt, uavhengig av avsender, mottaker, utstyr, applikasjon, tjeneste eller innhold. Årlig rapportering om nettnøytralitet er en lovpålagt oppgave for Nkom basert på forordningen om nettnøytralitet.

Rapportens hoveddel 2 beskriver status for kjernefunksjonene til internett i Norge, og dekker funksjoner som infrastruktur, trafikkutvikling, samtrafikk, overgangen fra IPv4 til IPv6, samt domenenavnsystemets oppslagstjenere og katalogtjenere. Årets rapport etablerer en basis for å kartlegge utviklingen av internetts kjernefunksjoner i årene fremover.

Nulltaksering i Norge

Gjennom de fem årene nettnøytralitetsforordningen har fungert, har Nkom fulgt utviklingen av nulltaksering tett. De første årene økte utbredelsen for hvert år, mens i år er det en nedgang. Samtidig har andelen sluttbrukere med stor datakvote økt de senere årene, noe som begrenser effekten av nulltaksering. Basert på en totalvurdering mener Nkom at nulltakseringen ikke har signifikante skadelige effekter i det norske markedet i dag.

BERECs retningslinjer for nettnøytralitet som Nkom benytter til regulatorisk vurdering av nulltaksering, revideres i år på bakgrunn av nye dommer fra EU-domstolen. Som en konsekvens av dette vil nulltaksering fases ut av markedet innen utgangen av 2022.

Nettnøytralitet og sikkerhet

Nkom observerer en noe økende utbredelse i tilbudet av sikkerhetsbeskyttelse for internettilgang. Dette er en påregnelig utvikling, tatt i betraktning omfanget av skadevare, svindel og andre sikkerhetstrusler på internett. I tillegg til de to konkrete tjenestetilbudene Telenor «Nettvern» og GlobalConnect «SafeSurf» vil Nkom følge denne utviklingen fremover. Nkom publiserte i november 2021 et prinsippnotat som drøfter avveining mellom nettnøytralitet og DNS-blokkering, med nærmere veiledning for internettilbyderne.

Kvalitet på internettilgangstjenesten

Nkom følger utviklingen av kvalitet på internettilgangstjenesten i det norske markedet. Det er en klar positiv utvikling i hastighet for fast internettilgang. Gjennomsnittlig hastighet for nedlasting og opplasting for fast internettilgang har økt med henholdsvis 19 % og 22 % siden i fjor. Det er også en positiv utvikling i hastighet for internettilgang via mobilnett. Det ser ut til at mobiltilbyderne er i stand til å møte etterspørselen.

For 4G har gjennomsnittlig nedlastingshastighet økt med 34 % siden i fjor, mens hastighet for opplasting har hatt en marginal økning. For 5G i Norge i 2021 var gjennomsnittlig nedlastingshastighet 365 Mbit/s (4G: 65 Mbit/s), gjennomsnittlig opplastingshastighet 39 Mbit/s (4G: 14 Mbit/s) og gjennomsnittlig forsinkelse 28 ms (4G: 44 ms). Foreløpig står 5G-trafikk for en liten andel av totalen, og det blir interessant å se om nettene holder tritt når dekningen bygges ut og flere kunder får håndsett som er 5G-klare.

1
Status for nettnøytralitet i Norge

Internettsamtrafikk

En viktig kjernefunksjon for internett er samtrafikk. I Norge utveksler internettaktørene trafikk mellom sine nett på samtrafikkpunkter som hovedsakelig er lokalisert i Oslo. Mesteparten av trafikken utveksles på private samtrafikkpunkter. I tillegg kobler den offentlige samtrafikkinfrastrukturen Norwegian Internet eXchange (NIX) sammen mer enn 70 små og store internettaktører.

Samtrafikk på internett i Norge er under utvikling. I møte med mer lukkede løsninger drevet frem av store datasenter- og plattformtilbydere, mener Nkom det er viktig å videreutvikle åpne, nøytrale og regionale samtrafikkløsninger. Dette har både konkurransemessige og sikkerhetsmessige fordeler.

Overgang fra IPv4 til IPv6

I 2022 har Norge en IPv6-utbredelse på 22,2 %, og rangerer med dette på 35 plass i verden. I oktober 2020, var Norge på 29. plass med utbredelsen 18,1 %. Norge har altså falt 6 plasser på listen i løpet av 1½ år. Samtidig har prosentandel for IPv6-utbredelse forbedret seg og økt med ca. 4 prosentpoeng. På europeisk nivå ligger Norge på 14. plass.

Dette vil si at internettaktørene i en del andre land øker IPv6-utbredelsen raskere enn det norske markedet. Nkom følger utviklingen videre og understreker viktigheten av at aktørene i det norske markedet legger til rette for bruk av IPv6 i størst mulig grad.

Utvikling av domenenavnsystemet

Det er nylig tatt i bruk nye metoder for domeneoppslag, såkalt «kryptert DNS». Én av disse metodene er DoH (DNS-over-HTTPS). Dagens tilbydere av DoH-oppslagstjenere ligger i hovedsak utenfor norsk jurisdiksjon. Det foreligger flere regulatoriske konsekvenser ved økende bruk av åpne oppslagstjenere, blant annet at myndighetsutøvelse basert på filtrering av DNS-oppslag håndheves i mindre grad.

EU har iverksatt initiativet DNS4EU som skal etablere et europeisk alternativ til de store amerikanske åpne DNS-oppslagstjenerne. Nkom vil fremover følge utviklingen av DNS4EU etter hvert som løsningen blir tilgjengelig og vurdere muligheten for norsk involvering og tilrettelegging for bruk av tjenesten for norske borgere. En slik tilnærming vil på sikt kunne bidra til å styrke posisjonen til DNS-oppslagstjenere innen europeisk jurisdiksjon.

Internettbaserte tjenester og plattformer

Økende bruk av internettbaserte tjenester og plattformer utfordrer eksisterende lovverk og fordrer tilpasning av lovverket. Innen EU etableres det i disse dager en pakke med regelverk som blant annet Digital Services Act og Digital Markets Act. Disse er EØS-relevante og vil dermed kunne bli del av norsk lov. Nytt regelverk vil legger premisser for forbrukernes og virksomhetenes bruk av internett.

Reguleringen av internettbaserte tjenester og plattformer forutsetter et tverrsektorielt samarbeid mellom myndighetsorganene. Dette for å sikre effektiv og enhetlig myndighetsutøvelse overfor ressurssterke aktører som spiller en dominerende rolle innen internetts økosystem. Nkom vil ta en aktiv rolle i dette samarbeidet på bakgrunn av vår kompetanse som regulatør av elektroniske kommunikasjonstjenester generelt, og regulering av nettnøytralitet og forhåndsdefinerte markeder spesielt.

1.1 Innledning og bakgrunn

Hoveddel I av årsrapporten beskriver status for nettnøytralitet i Norge. Dette er første året hvor rapporteringen om nettnøytralitet inngår i en bredere rapport om status for Internett i Norge. Nettnøytralitet er prinsippet om at internettrafikk skal behandles likt, uavhengig av avsender, mottaker, utstyr, applikasjon, tjeneste eller innhold. Denne rapporten dekker perioden 1. mai 2021 til 30. april 2022.

Nettnøytralitet ble lovfestet i Norge fra mars 2017 i forbindelse med innføringen av felleseuropeiske regler for nettnøytralitet, i henhold til forordning 2015/2120[1]. Formålet med forordningen er «å etablere felles regler som sikrer lik og ikke-diskriminerende håndtering av trafikk for internettilgangstjenester, samt tilhørende sluttbrukerrettigheter. Formålet er å beskytte sluttbrukerne og samtidig å garantere at internetts økosystem fortsetter å fungere som en motor for innovasjon.»[2]

Regulatorisk oppfølging av nettnøytralitet baseres også på BERECs retningslinjer om nettnøytralitet, som er etablert med hjemmel i forordningens artikkel 5(3). Ifølge fortalens punkt 19, skal regulatørene legge til grunn («take utmost account of») BERECs retningslinjer ved anvendelse av forordningen.

Hoveddel 1 av rapporten har følgende struktur: Kapittel 2 beskriver tilgang til et åpent internett via norske tilbyderes internettilgangstjenester og redegjør bl.a. for vurderinger av eksisterende nulltakseringstilbud. Kapittel 3 beskriver forhold knyttet til teknisk trafikkstyring i norske tilbyderes nettverk. Kapittel 4 beskriver forhold knyttet til sikkerhetstiltak for internettilgangen som tilbys. Kapittel 5 beskriver hvordan norske tilbydere informerer om internettilgangen de tilbyr. Kapittel 6 beskriver kvaliteten som oppnås for norske internettilgangstjenester, analysert basert på målinger med Nkom sin måletjeneste Nettfart.

Til sist gir kapittel 7 en samlet vurdering av status for nettnøytralitet i Norge. Dette kapitlet fungerer også som en overordnet oppsummering av innholdet i hoveddel 1 av rapporten.

[1] Europaparlamentets- og rådsforordning nr. 2015/2120

[2] Forordning 2015/2120, fortalens første avsnitt

1.2 Nulltaksering i Norge

I det norske markedet er det ikke tegn til introduksjon av nulltaksering for nye applikasjonskategorier. Andelen sluttbrukere med stor datakvote fortsetter å øke, noe som begrenser effekten av nulltaksering Utbredelsen av nulltaksering har falt i rapporteringsperioden. Samtidig strømmes nulltaksert musikk i økende grad av brukere med relativt store datakvoter. Basert på en totalvurdering av disse utviklingstrekkene mener Nkom at nulltakseringen i det norske markedet ikke har signifikante skadelige effekter.

BERECs retningslinjer for nettnøytralitet som Nkom benytter til regulatorisk vurdering av nulltaksering, revideres i år på bakgrunn av nye dommer fra EU-domstolen. Som en konsekvens av dette vil nulltaksering fases ut av markedet innen utgangen av 2022.

Nulltaksering er en form for prisdiskriminering av utvalgte applikasjoner sammenlignet med øvrige applikasjoner. Et typisk eksempel er at musikkstrømming kan benyttes uten at det forbrukes av sluttbrukerens avtalte datakvote. Det er internettilbyderen som beslutter hvilke applikasjoner som nulltakseres.

Regulatorisk vurdering av nulltaksering utføres som en helhetsvurdering basert på kriteriene som fremgår av BERECs retningslinjer om nettnøytralitet. Ettersom retningslinjene revideres i år, vil fremtidig vurdering av nulltaksering være basert på andre kriterier enn de som har vært benyttet de senere årene.

1.2.1 Internettilbydernes markedsposisjon

Nkom har tidligere vurdert nulltakseringstilbud fra både Telenor[3] og Telia[4]. Begge har navnet «Music Freedom», og omfatter nulltaksering av utvalgte tilbydere av musikkstrømming. Nkom har i disse sakene uttrykt bekymring for at tilbudene kan ha negative effekter, grunnet de to internettilbydernes betydelige markedsposisjon og mulige påvirkningskraft.

Ekomstatistikken for 2021 viser at den duopolistiske situasjonen fortsetter ettersom Telenor og Telia til sammen har om lag 79 % av abonnentene i markedet for telefonikoblede mobiltjenester. Etter omsetning har selskapene til sammen om lag 84 % av det private markedet og 91 % i bedriftsmarkedet.

1.2.2 Effekt på innholdstilbyderne

Nkom mener generelt sett at nulltakseringstilbudene kan påvirke konkurranseforholdene i innholdsmarkedet. Dette fordi bruken av utvalgte musikkapplikasjoner, på grunn av den positive prisdiskrimineringen, kan synes mer fordelaktig for brukerne enn ved bruk av andre applikasjoner hvor overføringen av innholdet spiser av datakvoten.

3 | Vurdering av Telenors nulltakseringstilbud

4 | Vurdering av Telias nulltakseringstilbud

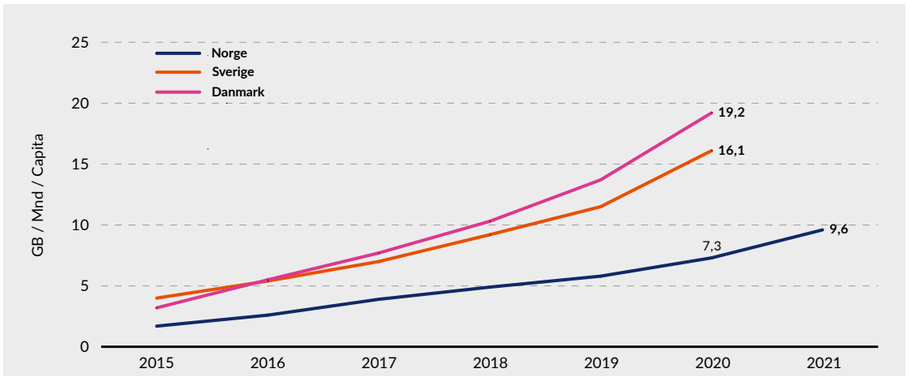
Telenor og Telias tilbud av den nulltakserte tjenesten «Music Freedom» inneholder musikkstrømme-tjenester fra Spotify, Tidal, Beat, Apple Music, Deezer og Audiomack. I tillegg inngår SoundCloud i Telenors tilbud. Nkom opprettholder vår tidligere vurdering om at omfanget av innholdstilbydere som i realiteten er inkludert i nulltakserings-ordningene, er relativt begrenset og hovedsakelig omfatter store, veletablerte tilbydere.

Når det gjelder utviklingen av nulltaksering av musikkstrømming i Norge de senere årene, er antall musikkstrømmeapplikasjoner relativt stabilt. Nkom har ikke mottatt henvendelser om problemer med inkludering i nulltakseringsordningene i inneværende rapporteringsperiode.

1.2.3 Effekt på sluttbrukerne

Nkom mener at nulltakseringstilbudene kan påvirke sluttbrukernes reelle valgfrihet, særlig sett i lys av at datakvoter i Norge er relativt små og relativt høyt priset sammenliknet med våre naboland. Når den inkluderte datakvoten som kan brukes fritt er relativt liten, blir nulltaksering mer problematisk enn tilfellet ville vært med større datakvoter.

Nkom observerer at norske mobilabonnenter i flere år har hatt det laveste forbruket av data ifølge nordisk-baltiske statistikkinnsamling. I land hvor ubegrenset inkludert datamengde er mer utbredt, vil nulltaksering være mindre problematisk. Figur 1 nedenfor viser samlet dataforbruk for mobil internettilgang i Norge sammenlignet med Sverige og Danmark:



Figur 1: Samlet dataforbruk i mobilnett per måned per innbygger målt i gigabyte (GB)

Norge er blant de landene som har et relativt lavt dataforbruk i mobilnett, og samtidig relativt høye priser på abonnement med ubegrenset datakvote. Dette impliserer at nulltaksering er mer problematisk i Norge. Når datakvotene er store nok, vil tilbud om nulltakserte tjenester i liten grad påvirke brukernes valg.

Mobilabonnement med høyere datakvote er mer utbredt i flere andre land enn Norge. Tabell 1 nedenfor viser andelsfordelingen av samlet kundemasse (i privatmarkedet) per datakvote i Norge ved utgangen av hvert år i perioden fra 2017 til og med 2021.

Kvotestørrelse	2017	2018	2019	2020	2021
Ingen data inkludert	23,1 %	19,3 %	16,5 %	14,0 %	14,2 %
Fra 0 til 1 inkludert	7,2 %	7,6 %	6,0 %	6,4 %	5,1 %
Fra 1 til 5 inkludert	45,6 %	43,7 %	45,2 %	41,2 %	33,0 %
Fra 5 til 10 inkludert	16,2 %	16,3 %	16,6 %	17,5 %	15,6 %
Fra 10 til 20 inkludert	6,5 %	6,6 %	7,5 %	9,9 %	14,8 %
Over 20 inkludert	1,5 %	6,4 %	8,2 %	–	–
Fra 20 til 100 inkludert	–	–	–	5,3 %	7,7 %
Over 100 inkludert	–	–	–	5,7 %	9,6 %

Tabell 1: Fordelingen av samlet kundemasse (privat) per månedlig datakvote

Den største gruppen av norske sluttbrukere har fortsatt abonnement med en datakvote på mellom 1 GB og 5 GB. Andelen sluttbrukere med datakvote i dette intervallet har imidlertid falt betydelig fra 2020 til 2021. Trenden peker i retning av at andelen sluttbrukere som har kvoter større enn 10 GB per måned, er økende. Økningen i 2021 er noe større enn økningen i årene før. Den største økningen i 2021 har skjedd for abonnementer med datakvote på mellom 10 GB og 20 GB.

I løpet av det siste året, er abonnement med såkalt «fri» databruk, altså kvoter over 100 GB, blitt noe mer utbredt. Nkom observerer også at trenden i markedet viser at store datapakker er blitt noe billigere siden fjorårets nettnøytralitetsrapport. Nkom ser på dette som en mulig konsekvens av reguleringen i mobilmarkedet som trådte i kraft 14. mai 2020.

1.2.4 Utbredelse av nulltaksering

Med økende utbredelse av nulltaksering øker omfanget av sluttbrukere som oppmuntres til å bruke noen utvalgte innholdstilbydere. Utbredelsen av nulltaksering ble imidlertid i fjorårets årsrapport vurdert til å være begrenset. Dette var hovedårsaken til at Nkom, ut fra en totalvurdering, fant at det ikke var grunnlag for å gi pålegg om retting av nulltakseringstilbudene i markedet.. Fortsatt er det slik at nulltakserte tjenester bare omfatter Telenor og Telias tilbud om «Music Freedom».

- Telias nulltakseringstjeneste «Music Freedom» er inkludert i Telia X-abonnementene, og for Telia Mobil-kunder som er under 29 år (unntatt Barn-abonnement). «Music Freedom» er også inkludert i Mobilt Bredbåndsabonnementene 50 GB, 100 GB, 200 GB og 500 GB. Andre kunder kan kjøpe tjenesten for 29 kr per måned. Tjenesten gjelder kun strømming av musikk og nedlasting av spillelister[5].
- Telenors nulltakseringstjeneste heter også «Music Freedom» og er inkludert i Fleksi-, Yng- og U18-abonnementene. Produktet kan kjøpes separat for 49 kr i måneden av de som har Next-, Original-, Medium-, Trygg- eller Trygg Start-abonnement.

5 | Telia Music Freedom

Andelen privatabonnement med «Music Freedom» har i rapporteringsperioden falt fra om lag 34 % til 32 %. Selv om både Telenor og Telia tilbyr muligheten for å kjøpe «Music Freedom» separat for henholdsvis 49,- og 29,- til enkelte andre abonnement, bidrar dette i liten grad til kundemassen som har «Music Freedom». Telia rapporterer at om lag halvparten av kundene med «Music Freedom» har Telia X-abonnement. Telia X er et abonnement med «fri databruk» og det vil derfor gjøre nulltakseringen mindre relevant.

Samlet for Telenor og Telias kundemasse har andelen privatabonnement med nulltaksering per månedlig datakvote utviklet seg som vist i nedenstående tabell:

Kvote	April 2018	April 2019	April 2020	April 2021	April 2022
0 - 1 GB[6]	0 %	1,1 %	1,2 %	1,6 %	1,4 %
1 - 5 GB	16,3 %	17,1 %	20,2 %	12,3 %	10,5 %
5 - 10 GB	49,9 %	33,3 %	26,6 %	21,9 %	20,8 %
> 10 GB	33,6 %	48,3 %	52 %	64,3 %	67,3 %

Tabell 2: Andel privatabonnement med nulltaksering per månedlig datakvote

Som vist i tabellen over, har en økende andel av privatkundene med «Music Freedom» et abonnement med en månedlig datakvote på 10 GB eller mer. En slik utvikling reduserer i noen grad de negative effektene ved nulltakserte tjenester.

Ifølge informasjon fra Telenor og Telia om gjennomsnittlig forbruk av nulltaksert innhold, er det sluttbrukere med datakvoter større enn 10 GB per måned som har høyest gjennomsnittlig dataforbruk av «Music Freedom». Også dette forholdet er med på å redusere de negative effektene ved nulltakserte tjenester.

1.3 Trafikkstyring og spesialiserte tjenester

Nkoms informasjonsinnsamling fra internettilbyderne viser ikke signifikante endringer sammenlignet med i fjor når det gjelder trafikkstyring av internettilgangstjenesten og tilbudet av spesialiserte tjenester i markedet. Nkom har ikke gjennomført detaljert gransking av rapporterte trafikkstyringstiltak eller spesialiserte tjenester, men legger til grunn at disse tilbys i overensstemmelse med forordningen. I fremtiden vil Nkom kunne iverksette mer utførlige undersøkelser av tiltakene.

1.3.1 Trafikkstyring av internettilgangen

Som en del av datainnsamlingen til den årlige ekomstatistikken, har Nkom har innhentet informasjon om trafikkstyring av internettilgangen fra norske internettilbydere. Dette er i tråd med BERECs anbefaling. Årets resultater viser ingen signifikant forskjewll fra fjorårets resultater. Ifølge innhentet informasjon, er typiske trafikkstyringstiltak blokkering av domenenavn i DNS etter rettslig pålegg, Kripos Child Abuse Filter, blokkering av TCP/UDP-porter ved spesifikke sikkerhetstiltak (f.eks. for å forhindre DDoS og andre former for dataangrep).

6 | Abonnement uten datakvote inkludert, som kontantkort, vil ved kjøp av datapakke på 10, 15 eller 20 GB inkluderes i tallene for den kalendermåneden datapakkene er kjøpt.

I det norske markedet ble det i mars 2021 for første gang observert hastighetsdifferensiert internettilgang da Telenor lanserte «Next». I desember 2021 lanserte Telia tilsvarende tjenester med «Telia X». BEREC beskriver i sine retningslinjer at slike abonnement er i tråd med forordningen så lenge abonnementene er applikasjons-agnostiske, det vil si at alle applikasjoner behandles med lik trafikkstyring.

1.3.2 Spesialiserte tjenester

Nkom har også innhentet informasjon om spesialiserte tjenester. Det vil si andre tjenester som tilbys i parallell med internettilgangstjenester og som oppfyller spesifikke kriterier i forordningen. Dataene viser at typiske spesialiserte tjenester i fastnett er IP-telefoni og IPTV. I mobilnett er VoLTE relativt vanlig å tilby. Dette samsvarer med typiske eksempler på spesialiserte tjenester i BERECs retningslinjer for nettnøytralitet.

Nkom stilte også spørsmål om hvordan tilbyderne sikrer at kapasiteten i nettverket er tilstrekkelig til at de spesialiserte tjenestene ikke går ut over den allmenne kvaliteten på internettilgangen til sluttbrukerne. Det gjennomgående svaret på dette er at trafikken på forbindelsene i nettet overvåkes kontinuerlig og at kapasiteten bygges ut ved behov.

Nkom har ikke gjennomført nærmere undersøkelser av de rapporterte trafikkstyringstiltak og spesialiserte tjenestene, men legger til grunn at disse tilbys i overensstemmelse med forordningen. I fremtiden vil Nkom kunne iverksette mer utførlige undersøkelser av tjenester som tilbys i det norske markedet.

1.4 Nettnøytralitet og sikkerhet

Nkom observerer økende utbredelse i tilbudet av sikkerhetsbeskyttelse for internettilgang. Dette er en påregnelig utvikling, tatt i betraktning omfanget av skadevare, svindel og andre sikkerhetstrusler på internett. I tillegg til de to konkrete tjenestetilbudene Telenor «Nettvern» og GlobalConnect «SafeSurf» vil Nkom følge denne utviklingen fremover, og om nødvendig innlede dialog med tilbydere om de regulatoriske rammene for slike produkt. Nkom publiserte i november 2021 et prinsippnotat som drøfter avveining mellom nettnøytralitet og DNS-blokkering, med nærmere veiledning for internettilbyderne.

1.4.1 Sikkerhetsunntaket i forordningen

Det fremgår av forordningen artikkel 3(3)b at trafikkstyringstiltak utover rimelig trafikkstyring ikke er tillatt, med mindre det er nødvendig av hensyn til sikkerhet og integritet i nettverket. Unntaket omtales gjerne som «sikkerhetsunntaket» og praktiseringen av unntaket skal være basert på en «streng fortolkning», jf. fortale 11 i forordningen. Videre skal aktuelle tiltak bare finne sted så lenge som nødvendig.

Sikkerhetsunntaket er videre presisert i BERECs retningslinjer, punkt 83-87. Blant annet beskriver retningslinjene hvilke sikkerhetstrusler som er aktuelle å beskytte imot, og hvordan nasjonale regulatører kan gå frem i vurderingen av om sikkerhetstiltak er berettiget. Det understrekes i retningslinjene at sikkerhetsunntaket kan benyttes som basis for omgåelse av regelverket og at regulatører derfor bør vurdere nøye om forordningen er oppfylt i vurderingen av aktuelle produkt og tjenester i de nasjonale markedene.

Nkom har i forkant av, og underveis i arbeidet med årsrapporten fokusert på DNS-baserte sikkerhetstiltak hos norske internettilbydere. Dette er tiltak som aktualiserer spørsmålet om hvorvidt sikkerhetsunntaket i forordningen kommer til anvendelse, og om tiltakene i så fall er lovlige i henhold til forordningens bestemmelser og BERECs retningslinjer. Under presenteres to relevante tjenester som tilbys av internettilbydere i det norske markedet.

1.4.2 Sikkerhetsfilter i det norske markedet

Telenor «Nettvern»

Telenor Norge AS tilbyr sikkerhetstjenesten «Nettvern», som ifølge selskapet blokkerer nettsteder som er infiserte eller falske. Dette ved hjelp av et filter som forhindrer sluttbrukeren fra å gå inn på nettsteder som inneholder virus, svindelforsøk eller skadelig programvare. I stedet for å bli sendt til denne siden mottar sluttbrukeren et varsel om at man er i ferd med å åpne en usikker nettside.

«Nettvern» består videre av et sikkerhetsfilter som er automatisk aktivert i alle faste og mobile internettilgangstjenester, men sluttbrukeren kan slå det av dersom man ønsker. Videre gjennomføres filtreringen gjennom blokkeringer i DNS.

Telenor har en nærmere beskrivelse av tjenesten på sine nettsider.

GlobalConnect «SafeSurf»

GlobalConnect AS tilbyr sikkerhetstjenesten «SafeSurf», som ifølge selskapet beskytter brukere og systemer fra å komme i kontakt med skadelige nettsider som inneholder virus eller brukes til svindelforsøk, såkalt phishing. Når tjenesten er aktivert blokkerer den automatisk tilgang til skadelige sider og domener, og sender brukeren videre til en sikker side.

«SafeSurf» er ifølge GlobalConnect automatisk aktivert hos kunder som per i dag har internett via fiber (med fast IP-adresse) eller xDSL (enten med fast IP-adresse eller tilleggstjenesten Wi-Fi Connect). Tjenesten kan også tilbys andre abonnementstyper, eller der hvor sluttbrukeren konfigurerer DNS selv.

GlobalConnect har en nærmere beskrivelse av tjenesten på sine nettsider.

1.4.3 Veiledning for internettilbyderne

På bakgrunn av den kunnskap som Nkom har på rapporteringstidspunktet, vurderes det at det ikke er grunnlag for pålegg eller andre inngrep i markedet. Nkom ønsker likevel å gi en generell veiledning om hvordan DNS-baserte sikkerhetstiltak bør tilbys til norske sluttbrukere.

For vanlige internettbrukere er forhåndsaktivert DNS-filter rimelig effektivitet som sikkerhetstiltak. Dette er fordi mesteparten av internettkommunikasjon gjennomfører DNS-oppslag før kommunikasjonen utføres. Men samtidig oppstår det en risiko for overblokkering/«falske positiver» fordi domener med rettmessig innhold kan blokkeres i sin helhet på grunn av infiserte eller andre skadelige enkeltsider.

Nkom mener at det her må sondres mellom forhåndsaktivert DNS-filter, valgfritt DNS-filter og sikkerhetsprogramvare installert på sluttbrukerens PC. De to sistnevnte løsningene vil uten videre kunne tas i bruk uten å være i strid med sikkerhetsunntaket i forordningen. Forhåndsaktiverte filter forutsetter imidlertid særlig god transparens og informasjon til sluttbruker om hva tjenesten går ut på. Videre må tilbyder ha en god og etterprøvbar oversikt over blokkeringslister og hvilke blokkeringer som utgjør en reell trussel i henhold til kravene i regelverket.

Nkom ønsker her å presisere at det er adgang til å be om innsyn i hvilke konkrete vurderinger tilbyderen har gjort for sine spesifikke blokkeringer, jf. forordningen artikkel 5 (2).

Nkom publiserte et prinsippnotat om DNS-baserte sikkerhetstiltak i november 2021, som utdyper momentene som er nevnt over. Notatet er tilgjengelig på våre nettsider.

1.5 Informasjon om internettilgangstjenesten

Nkoms vurdering er at norske tilbydere generelt informerer godt om internettilgangstjenesten, både når det gjelder trafikkstyring og hastighet for fast og mobil internettilgang. Nkom har ikke gjennomført en detaljert gjennomgang av alle tilbyderes nettsider og kontraktsvilkår, men legger til grunn at informasjon publiseres i henhold til kravene i forordningen og at tilbyderne gjør selvstendige vurderinger når de endrer eksisterende tjenester eller lanserer nye. Nkom vil i fremtiden kunne gjøre mer konkrete vurderinger i enkeltsaker, for eksempel knyttet til fast trådløs internettilgang og hvorvidt tilbyderen plikter å opplyse om normalt tilgjengelig hastighet.

1.5.1 Krav om informasjon

Krav til informasjon om internettilgangstjenesten som tilbydere skal gjøre tilgjengelig for sine sluttbrukere fremgår av forordningen artikkel 4. Artikkel 4 (1) oppstiller krav til åpenhet og transparens i avtalene mellom tilbyder og sluttbruker, mens artikkel 4 (2) regulerer tilbyders plikt til transparente, enkle og effektive klagebehandlingsprosedyrer.

Nkom har gjort en gjennomgang av aktuelle tilbyderes nettsider og vurdert etterlevelsen av artikkel 4 i Forordningen. I det følgende knyttes det noen kommentarer til gjennomgangen.

1.5.2 Informasjon om trafikkstyring

Tilbydere av internettilgangstjenester plikter å informere om hvilke trafikkstyringstiltak som brukes. Aktuelle trafikkstyringstiltak er nærmere beskrevet i delkapittel 3.1.

Ifølge forordningen skal tilbyderne informere om tiltakene i avtalevilkårene og gjøre disse offentlig tilgjengelige, typisk på tilbyderens nettside. Selv om tilbyderne kan dokumentere at informasjonen offentliggjøres, er det også relevant å vurdere innhold og kvalitet på informasjonen.

Nkoms gjennomgang i forbindelse med årsrapporten viser at tilbyderne har en varierende, men generelt tilfredsstillende fremstilling av trafikkstyringstiltak. Enkelte tilbydere har dedikerte sider om nettnøytralitet, hvor trafikkstyring er ett av flere tema. Andre tilbydere informerer mer direkte om trafikkstyring i vilkår og på nettsidene. Dedikerte temasider gir sluttbrukere mer helhetlig informasjon om nettnøytralitet, men begge løsninger omtalt i dette avsnittet er etter Nkoms oppfatning i overensstemmelse med regelverket.

1.5.3 Informasjon om hastighet

Fast internettilgang

Det følger av forordningen artikkel 4 (1) (d) at sluttbruker skal informeres om hastigheten som tilbyderen realistisk sett er i stand til å levere. Tilbydere av fast internettilgang skal angi følgende måleparametere for hastighet, ved både ned- og opplastning:

- minimumshastighet
- normalt tilgjengelig hastighet
- maksimumshastighet
- markedsført hastighet

Med «normalt tilgjengelig hastighet» menes hastigheten som en sluttbruker kan forvente å oppnå mesteparten av tiden vedkommende bruker tjenesten. Det er sannsynligvis denne måleparameteren som gir sluttbruker mest relevant informasjon om internettilgangens ytelse.

Med hensyn til forordningens krav om åpenhet og transparens, anser BEREC visse typer fast trådløs tilgang (Fixed Wireless Access) som fast internettilgang Dette omfatter for eksempel tilfelle der trådløs teknologi (inkludert mobil) brukes til internettilgang på et fast sted med dedikert utstyr og enten bruker kapasitetsreservering eller dedikerte frekvensbånd. I slike tilfeller bør krav til tilgjengeliggjøring av informasjon i kontrakter og på tilbyderens nettsider være i samsvar med kravene som gjelder for fast internettilgang. Etter det Nkom kjenner til, benyttes ikke kapasitetsreservering eller dedikerte frekvensbånd for fast trådløs tilgang hos norske internettilbydere per utgangen av april 2022.

Samtidig observerer Nkom at det blir stadig mer aktuelt med utrulling av nye tjenester via fast trådløs tilgang. Nkom kan derfor i enkeltsaker vurdere at en tjeneste blir å anse som en fast internettilgang på bakgrunn av konkret implementasjon og betingelsene for det spesifikke tjenestetilbudet.

For fast internettilgang observerer Nkom at tilbyderne generelt opplyser om de ulike hastighetsparameterne som forordningen krever, inklusive normalt tilgjengelig hastighet.

Mobil internettilgang

I mobilnett er normalt tilgjengelig hastighet i en gitt celle vanskelig å forutse på grunn av det varierende antall aktive brukere. Av den grunn er det kun tilbydere av fast internettilgang som er pålagt å opplyse om denne hastighetsparameteren.

Forordningen krever imidlertid at tilbydere av mobil internettilgang angir følgende måleparametere for hastighet:

- anslått maksimumshastighet
- markedsført hastighet

Mobile internettilgangstjenester omfatter både vanlige mobilabonnement og dedikerte internettabonnement ettersom begge er tjenester som gir tilgang til internett. Vanlige mobilabonnement støtter både internettilgang og telefoni/SMS, mens dedikerte internettabonnement kun støtter tilgang til internett. Førstnevnte benyttes ofte via mobiltelefon, mens sistnevnte ofte benyttes via ruter.

Når de gjelder dedikerte internettabonnement i mobilnettet, skiller man ofte mellom «fast trådløs internettilgang» som tilbys på en fast geografisk lokasjon, ofte med fastmontert utendørs antenne, og «dedikert mobil internettilgang» som man kan benytte fritt på ulike geografiske lokasjoner innenfor dekningsområdet. Disse forskjellene kan gi opphav til ulike betingelser for oppnådd hastighet på internettilgangen for de ulike abonnementene.

Konklusjon

Nkoms gjennomgang viser at tilbyderne i varierende grad presenterer informasjonen om internettilgangstjenesten på en lettfattelig og tilgjengelig måte. Sluttbrukere bør derfor være bevisst hvilken informasjon man leter etter, eller kontakte sin tilbyder for å få konkret anvisning på hvor informasjonen er tilgjengelig. For hastighetsdifferensierte abonnement konstateres det en forbedret transparens når det kommer til differensiering/manglende differensiering av sluttbrukere ved metningssituasjoner i tilbyderens mobilnett. w

1.6 Kvalitet på internettilgangstjenesten

Det er positivt å se at hastighet for fast internettilgang fortsetter den gode trenden fra forrige rapporteringsperiode. Gjennomsnittlig hastighet for nedlasting og opplasting for fast internettilgang har økt med henholdsvis 19 % og 22 % siden forrige rapporteringsperiode.

Det er også en positiv utvikling i hastighet for internettilgang via mobilnett. Det ser ut til at mobiltilbyderne er i stand til å møte etterspørselen gjennom å bygge ut dekning og ta i bruk radioteknologier som effektivt utnytter tilgjengelig spektrum.

For 4G har gjennomsnittlig nedlastingshastighet økt med 34 % siden forrige rapporteringsperiode, mens gjennomsnittlig opplastingshastighet har hatt en marginal økning. For 5G i Norge i 2021 var gjennomsnittlig nedlastingshastighet 365 Mbit/s (4G: 65 Mbit/s), gjennomsnittlig opplastingshastighet 39 Mbit/s (4G: 14 Mbit/s) og gjennomsnittlig forsinkelse 28 ms (4G: 44 ms). Foreløpig står 5G-trafikk for en liten andel av totalen og det blir interessant å se om nettene holder stand når dekningen bygges ut og en større andel av kundene får terminaler som er 5G-klare.

1.6.1 Krav til kvalitet på internettilgangstjenesten

Artikkel 5 i forordningen sier at nasjonale myndigheter har overvåkings- og rapporteringsforpliktelser som skal sikre at tilbydere av internettilgangstjenester oppfyller sine forpliktelser vedrørende åpen internettilgang. I artikkel 5(1) angis plikt for nasjonale myndigheter om å følge opp tilbydernes etterlevelse av artikkel 3 og 4.

Fortalens avsnitt (17) understreker viktigheten av at spesialiserte tjenester og bruk av slike ikke skal føre til redusert generell kvalitet på kundens tilgang til internett. For tilgang til internett via mobilnettverk lempes det noe på kravene som følge av de særskilte forholdene knyttet til varierende antall aktive brukere pr. celle samt dekning som ikke er homogen. Men over tid forventer man også her at den generelle kvaliteten på internettilgangen opprettholdes.

Fra høsten 2021 har BEREC arbeidet med å oppdatere sin metodikk for beskrivelse av hvordan nasjonale myndigheter kan utføre, evaluere og publisere resultater fra kvalitetsmålinger i fast- og mobilnett. Den oppdaterte metodebeskrivelsen var ute på offentlig høring i starten av 2022. En viktig endring i den oppdaterte beskrivelsen er at den nå gir veiledning til nasjonale myndigheter for hvordan de kan følge med på utviklingen av generell kvalitet på internettilgangen. Kapittel 1.6.4 viser hvordan metodikken kan tas i bruk for å analysere generell kvalitet på internettilgangen.

1.6.2 Regulatorisk oppfølging

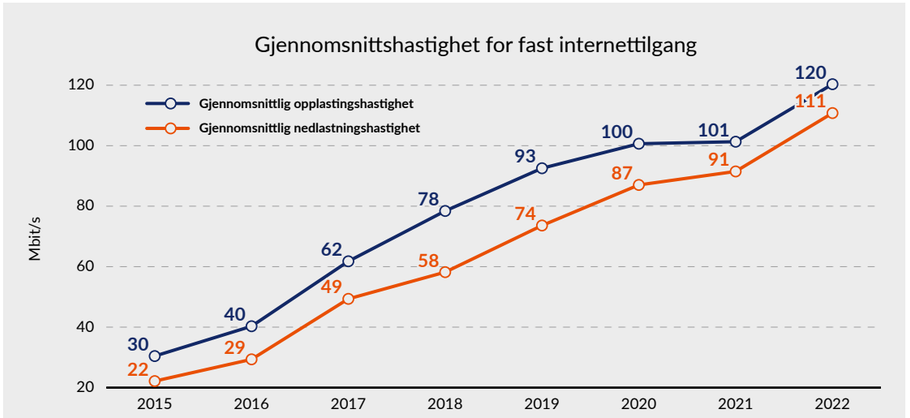
Et tiltak for oppfølging av artikkel 5(1) i forordningen er å følge utviklingen av kvalitet som sluttbrukerne måler på sin internettilgang. I denne rapporten har Nkom vurdert resultatene fra Nkoms måletjeneste Nettfart, som kan brukes via nettleser og/eller mobilapplikasjon. Nettfart baserer seg på nettdugnad (crowd-sourcing) ved at det er brukerne selv som aktivt gjør målinger og dermed produserer datagrunnlaget som Nkom analyserer. Nettfart.no har om lag 100 000 målinger pr måned, og nettfart mobilapp har om lag 20 000 målinger pr måned.

Som ved alle former for nettdugnad, kan det være noe begrenset hvor representativt det statistiske grunnlaget er. Måleresultatene gir imidlertid en indikasjon på hvor god ytelse sluttbrukerne opplever på sin internettilgang. Datagrunnlaget viser også at det over tid samles informasjon fra en svært stor andel av de norske tilbyderne.

1.6.3 Måleresultater

Måleresultater fra nettfart.no

I dette delkapitlet presenteres resultater fra målinger gjort via nettfart.no. For fast internettilgang presenteres utviklingen av gjennomsnittshastighet på tvers av ulike abonnement.



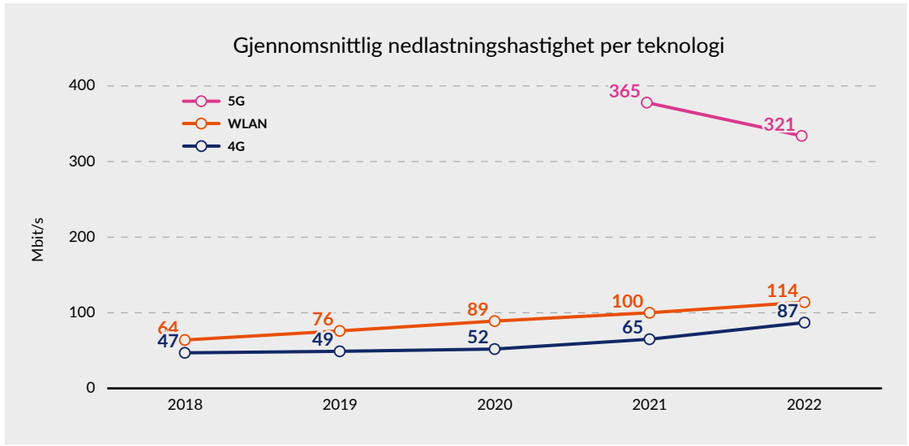
Figur 2: Gjennomsnittshastighet for fast internettilgang (kilde: nettfart.no)

Figur 2 viser at gjennomsnittlig målt nedlastningshastighet på tvers av sluttbrukernes ulike abonnement, hittil i 2022 er ca. tre ganger så høy som i 2016[7]. Veksten ser ut til å fortsette, og ligger på om lag 10-20 Mbit/s per år.

7 | I årets rapport brukes et noe mer omfattende datagrunnlag, enn hva som var tilfellet for fjorårets rapport. Trendene er likevel de samme.

Måleresultater fra nettfart mobilapp

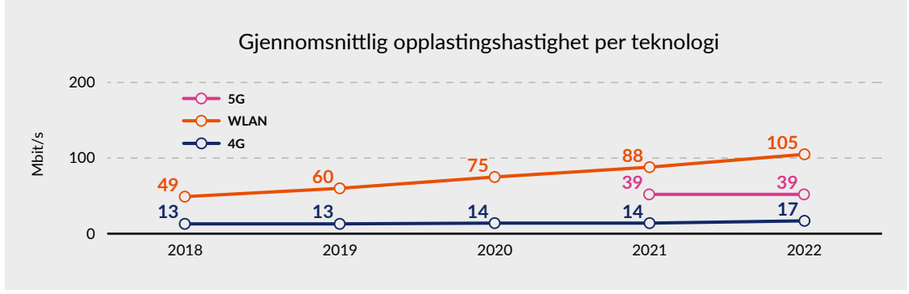
Her presenteres resultater målt via nettfart mobilapp, først gjennomsnittshastighet pr. teknologi (4G, 5G og WLAN), og til sist nøkkeltall for målinger via 5G utført av kunder i mobilnettene til Telenor og Telia i 2021.



Figur 3: Gjennomsnittlig nedlastningshastighet per teknologi (kilde: nettfart mobilapp)

Figur 3 viser gjennomsnittlig målt nedlastingshastighet, fordelt på teknologi. Figuren viser at brukerne av nettfart mobilapp oppnår betydelig høyere nedlastingshastighet når de måler via 5G, sammenlignet med målinger via 4G og WLAN. For 5G viser figuren en noe nedadgående trend, men det er vanskelig å si noe sikkert om årsaken til dette. Det kan være et resultat av aktivering av 5G i lavere frekvensbånd i takt med at tilbyderne skrur på teknologien også utenfor de store byene.

Gjennomsnittlig hastighet for 4G og WLAN er svakt økende. Det kan se ut til at 4G den siste tiden tar inn noe av differansen mot WLAN. Kanskje henger dette sammen med moderniseringen som gjøres i mobilnettene samtidig med at 5G aktiveres. For WLAN-målinger er det imidlertid usikkert hvilket transmisjonsmedium som benyttes til og fra boligen for den enkelte måling. Det kan være fiber, hybridkabel eller fast trådløst bredbånd.



Figur 4: Gjennomsnittlig opplastingshastighet per teknologi (kilde: nettfart mobilapp)

Figur 4 viser at det i mobilnettene er større forskjeller mellom gjennomsnittlig målt opp- og nedlastningshastighet, enn hva som observeres for målinger gjort via WLAN. En mulig forklaring er at WLAN i større grad er koblet til aksesslinjer med symmetriske egenskaper, slik mange fiberabonnement tilbyr.

Figuren viser også at gjennomsnittlig opplastingshastig via mobilnettene ligger på et mye lavere nivå enn hva tilfellet er for nedlastingshastigheter (Figur 3). Forklaringen er sannsynligvis at mobilnettene reserverer en større del av det tilgjengelige frekvensspektrumet til nedlasting, ettersom en antar at dette er den dominerende retningen for trafikk mellom internett og den enkelte kunde.

Nøkkeltall for SG-nettet i Norge for 2021 (Telenor og Telia)

Gjennomsnittlig nedlastningshastighet for 5G	Gjennomsnittlig opplastingshastighet for 5G	Gjennomsnittlig forsinkelse for 5G
365,00 Mbit/s	39,00 Mbit/s	28,27 ms
Maksimal registrert 5G nedlastningshastighet for Telenor	**Maksimal registrert 5G opplastingshastighet for Telenor**	**Minimal registrert 5G forsinkelse for Telenor**
907,43 Mbit/s	137,44 Mbit/s	9,95 ms
Maksimal registrert 5G nedlastningshastighet for Telia	**Maksimal registrert 5G opplastingshastighet for Telia**	**Minimal registrert 5G forsinkelse for Telia**
921,20 Mbit/s	159,04 Mbit/s	5,21 ms

Figur 5: Nøkkeltall for 5G-målinger i 2021 (kilde: nettfart mobilapp)

I Figur 5 viser vi utvalgte nøkkeltall for 5G-målinger i mobilnettene til Telenor og Telia i 2021. Gjennomsnittlig nedlastingshastighet, opplastingshastighet og forsinkelse for 5G-nettene i Norge i 2021 var henholdsvis 365 Mbit/s, 39 Mbit/s og 28 millisekund (ms). De registrerte målingene i Nettfarts databaser viser at Telia har noe høyere verdier når det gjelder de tre nevnte parametere. Målinger fra nettfart mobilapp viser uansett 5G-teknologiens potensiale for å tilby internettilgang med høye hastigheter og lav forsinkelse.

1.6.4 Generell kvalitet på internettilgangstjenesten

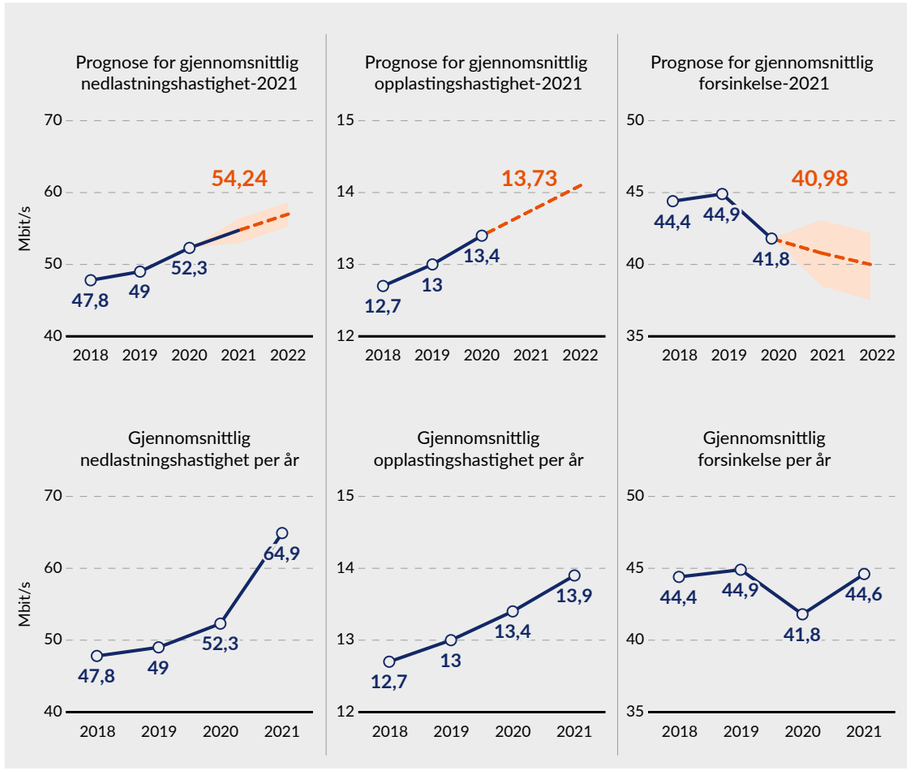
Nkom har anvendt BERECs nye metode for evaluering av generell kvalitet på internettilgangstjenesten på målingene gjort i 4G-nettene. Metoden benytter en prognosefunksjon basert på gjennomsnittlig nedlasting, opplasting og forsinkelse fra de foregående årene og bruker disse til å anslå forventninger til påfølgende år. Anslåtte og målte verdier kan deretter sammenlignes for å se om det finnes store avvik i resultatene.

Figur 6 viser prognoser for nedlasting- og opplastingshastighet samt forsinkelse for målinger gjort i 4G-nettene i Norge, i dette tilfellet aggregert for alle mobiloperatørene. Øvre del av figuren viser prognosen og nedre del viser de målte verdiene.

Prognose for gjennomsnittlig nedlastingshastighet for 2021 var 54 Mbit/s, samtidig som den målte verdien var 65 Mbit/s. Dette viser at utviklingen for nedlastingshastighet i 4G-nettet har vært mer positiv enn prognosen anslår, og at tilbyderne utvider kapasiteten etter behov.

Prognose for gjennomsnittlig opplastingshastighet for 2021 var 13,7 Mbit/s, samtidig som den målte verdien var 13,9 Mbit/s. Dette viser at utviklingen for opplastingshastighet i 4G-nettet har vært veldig tett på prognosefunksjonen sitt anslag.

Prognose for gjennomsnittlig forsinkelse for 2021 var 40,9 ms, og den målte verdien var 44,6 ms. En observerer her at målt forsinkelse har gått en del opp sammenlignet med prognosefunksjonen sitt anslag. For Nkom vil det være interessant å følge med på om denne trenden fortsetter neste år, eller om vi vil se en forbedring.



Figur 6: Prognoser for generell kvalitet på internettilgangstjenesten i 4G mobilnettene i 2021. Øverste del av figuren viser prognosene, mens nederste del viser oppnådd resultat. (kilde: nettfart mobilapp)

2
Internetts kjernefunksjoner i Norge

2.1 Innledning og bakgrunn

Hoveddel 2 av årsrapporten beskriver status for kjernefunksjonene til internett i Norge.

Rapporten er et oppdrag gitt av KDD til Nkom gjennom Stortingsmelding 28 (2020-2021) *Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester*.
I Stortingsmeldingens kapittel 10.8 heter det blant annet at «Regjeringen vil:

- At Nasjonal kommunikasjonsmyndighet publiserer en årlig statusrapport om *Internett i Norge*.
- Fortsette arbeidet for å bidra til at kjernefunksjonene til norsk internett er sikre og fremtidsrettede.»

Videre beskriver meldingen at «Nkom rapporterer årlig om nettnøytralitet i Norge, og denne statusrapporten bør videreutvikles til også å omfatte informasjon om utviklingen av kjernefunksjonene til norsk internett, internettforvaltning, internettbaserte tjenester og plattformer, samt eventuelle regulatoriske vurderinger i denne sammenheng.»

Hoveddel 2 er organisert etter følgende struktur: Kapittel 2 beskriver infrastruktur og trafikkutvikling for internett i Norge. Kapittel 3 drøfter utbredelse av IPv6 for internett i Norge. Kapittel 4 beskriver status for domenenavnsystemet og kryptert domeneoppslag.

Kapittel 5 beskriver anvendelsene av tingenes internett, inklusive sikkerhet for tingenes internett. Kapittel 6 drøfter internettsikkerhet for kjernefunksjonene, samt generelle sikkerhetstrender. Kapittel 7 omtaler lovverk knyttet til internettbaserte tjenester og plattformer.

Kapittel 8 beskriver utviklingen innen internasjonal internettforvaltning og norsk deltakelse i dette arbeidet. Til sist gir kapittel 9 en samlet vurdering av status for internett i Norge. Dette kapitlet fungerer også som en oppsummering av innholdet i hoveddel II av årsrapporten.

2.2 Infrastruktur og trafikkutvikling

En viktig kjernefunksjon for internett er samtrafikk. I Norge utveksler internettaktørene trafikk mellom sine nett på samtrafikkpunkter hovedsakelig lokalisert i Oslo. Mesteparten av trafikken utveksles på private samtrafikkpunkter. I tillegg kobler den offentlige samtrafikkinfrastrukturen Norwegian Internet eXchange (NIX) sammen mer enn 70 små og store internettaktører.

Samtrafikk på internett i Norge er under utvikling. I møte med mer lukkede løsninger drevet frem av store datasenter- og plattformtilbydere, mener Nkom det er viktig å videreutvikle åpne, nøytrale og regionale samtrafikkløsninger. Dette har både konkurransemessige og sikkerhetsmessige fordeler.

2.2.1 Utbredelse av internettilgangstjenesten

Nasjonal utbredelse av internettilgangstjenesten samsvarer i stor grad med utbredelsen av bredbånd. Nkoms dekningsundersøkelse for første halvår 2021 viser at nær 90 % av alle husstander hadde tilbud om bredbånd med minst 100 Mbit/s i nedlastingshastighet[8]. Dette er i hovedsak basert på fiber eller hybrid-nett, men også fast trådløst bredbånd bidrar.

8 | Bredbåndsdekning 2021 – nkom.no

Nesten alle husstandene som har tilbud om bredbånd med minst 100 Mbit/s nedlastingshastighet, har også tilbud om alternative tilknytninger. Det er geografiske ulikheter, men sett under ett har de fleste norske innbyggere gode muligheter for å koble seg til internett.

Ekomstatistikken for 2021[9] viser at Telenor, Altibox, Telia og GlobalConnect samlet hadde hånd om anslagsvis 85 % av markedet, når en slår sammen privat- og bedriftsmarkedet. I markedet for mobilabonnement er konsentrasjonen enda høyere. Samlet har Telenor, Telia og Ice/Altibox om lag 91 % av kundene. Disse tre selskapene er også de tre største aktørene i markedet for fast bredbånd, og står for en overveiende del av tilknytningene som gir norske brukere tilgang til internett.

2.2.2 Internettsamtrafikk i Norge

Samtrafikk er prosessen der ulike nett (autonome system) utveksler trafikk med hverandre. Dette er en viktig kjernefunksjon for internett. Hvor og hvordan slik trafikkutveksling skjer har betydning for både responstid, kvalitet og sikkerhet. Disse avveiningene har også en økonomisk side.

Samtrafikk
Det finnes to hovedmetoder for samtrafikk: *Peering* og *transit*. Ved peering utveksler to nett gjensidig trafikk mellom hverandre. Denne metoden benyttes typisk mellom internettilbydere som utveksler store trafikkvolum mellom sine nett. Ved transit betaler en internettilbyder en eller flere tredjepartstilbydere for å overføre trafikk til og fra resten av internett.

En skiller også gjerne mellom *nasjonal* og *internasjonal* samtrafikk, og mellom trafikkutveksling som skjer på *private* eller *offentlige* samtrafikkpunkt (Internet eXchange Points, IXP).

Mesteparten av samtrafikken mellom norske internettilbydere er geografisk sentralisert i Oslo, på private samtrafikkpunkter. I tillegg benyttes de offentlige samtrafikkpunktene NIX – Norwegian Internet eXchange[10]. NIX er en fellesbetegnelse for offentlige samtrafikkpunkter i Oslo, Stavanger, Bergen, Trondheim og Tromsø.

Samtrafikk via de offentlige samtrafikkpunktene er særlig viktig for mindre internettilbydere, og er en mulighet for å møte de store tilbyderne og utveksle trafikk med disse. Men også de større internettilbydere benytter NIX, som supplement til de private samtrafikkavtalene. Per første kvartal 2022 hadde NIX like under 70 kunder (tilkoblede nett).

2.2.3 Internettsamtrafikk mot utlandet

Det meste av internettrafikken mellom Norge og utlandet utveksles mellom samtrafikkpunkter i Oslo og de store internasjonale samtrafikkpunktene i Stockholm, Frankfurt, Amsterdam og London. Størstedelen av denne trafikken går imidlertid gjennom et begrenset antall forbindelser fra Oslo og via Sverige.

Nkom har siden 2016 påpekt behovet for å styrke den geografiske spredningen på rutingen av internettrafikk til og fra Norge på bakgrunn av nasjonal sikkerhet og beredskap. Dette blir stadig viktigere etter hvert som internettbaserte skytjenester, som gjerne produseres utenfor Norges grenser, utgjør en betydelig innsatsfaktor for sentrale samfunnsfunksjoner.

9 | Ekommarkedet helår 2021 – nkom.no
10 | nix.no

I perioden fra 2020 til 2022 er det etablert flere nye sjøfiberforbindelser til utlandet. Disse forbindelsene legger til rette for en voksende datasenternæring og økte behov for kapasitet og spredning. Staten har i perioden bidratt med nærmere 100 MNOK for å styrke sikkerheten på forbindelsene, og for å legge til rette for økt spredning av internettrafikken til og fra Norge.

Nye sjøfiberforbindelser til utlandet etablert siden 2020:

- Bulk, 2020: «Havfrue» fra New Jersey (USA) til Blaabjerg (Danmark) og Kristiansand
- Altibox, 2020: «Skagenfiber West» fra Larvik til Hirtshals (Danmark)
- Altibox, 2021: «NO-UK» fra Stavanger til Newcastle (Storbritannia)
- Bulk, 2022: «Havsil», fra Kristiansand til Hanstholm (Danmark)

Disse kommer i tillegg til de eksisterende sjøfiberforbindelsene til Tampnet mellom Vestlandet og Storbritannia, og Statnetts «Skagerrak 4» mellom Kristiansand og Tjele i Danmark.

Nkom vil fremover vurdere hvordan disse endringene bidrar til å styrke den geografiske spredningen og sikkerheten for internettsamtrafikken mot utlandet.[11] Spredning av trafikk vil her også være knyttet til utviklingen av internettbaserte tjenester og plattformer, og rollen til den norske datasenterindustrien.[12].

2.2.4 Utvikling for norsk internettrafikk

Nkom sendte i februar 2022 ut en spørring for å samle data om utviklingen av internettrafikk i både fast- og mobilnett. Utvalget omfattet de største internettilbyderne i begge disse kategoriene. På aggregert nivå og for perioden 2017 til første kvartal 2022 ser vi en årlig vekst på om lag 25-30 % for internettrafikk i både fast- og mobilnett.

Internettrafikk i mobilnettene

De siste to årene er trafikkveksten drevet av lanseringen av fast trådløst bredbånd. Trafikkutviklingen påvirkes av den teknologiske utviklingen og medfølgende økning i nettverkskapasitet, samt vekst i antall kunder og økte datakvoter. Datakvotene[13] for mobilabonnement har økt i de siste årene uten at prisene har økt tilsvarende.

Figur 7 viser utviklingen i internettrafikk fordelt på vanlige mobilabonnement, dedikerte internettabonnement[14] og gjesting i utlandet. Det er de vanlige mobilabonnementene som genererer mesteparten av internettrafikken i mobilnettene (over 80 %). I 2021 var internettrafikken i mobilnettene totalt 624 Petabyte (PB)[15], en økning på 32 % fra 2020.

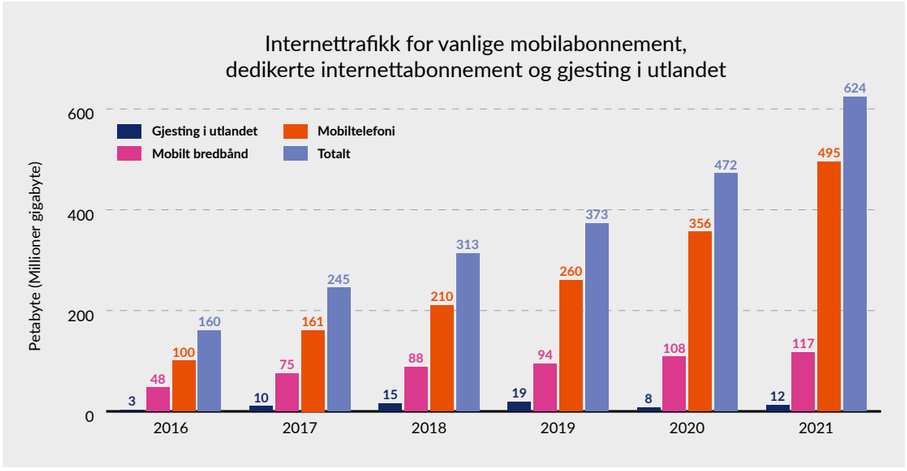
11 | Jf. målbilde 4 i rapporten «Robuste transmisjonsnett for Norge mot 2030», Nkom - 2022.

12 | Norske datasenter - berekraftige, digitale kraftsenter – regjeringen.no

13 | Den største gruppen av norske sluttbrukere har fortsatt abonnement med en inkludert datakvote på mellom 1 GB og 5 GB. Den største økningen i 2021 har skjedd for abonnementer med datakvote på mellom 10 GB og 20 GB.

14 | Dedikerte internettabonnement omhandler produkter som tilbyr en dedikert datatjeneste ved hjelp av eget SIM-kort. Brukeren får en ren dataforbindelse mellom terminalen og mobilnettet, og via denne tilgang til Internett.

15 | Petabyte (PB) er 1000 Terabyte eller 1000 000 Gigabyte.



Figur 7 - Internettrafikk for vanlige mobilabonnement, dedikerte internettabonnement og gjesting i utlandet

Mobiltilbyderne ruller nå ut 5G i stor skala. I første kvartal 2022 er om lag 25 % av tilkoblende håndsettene klargjort for denne teknologigenerasjonen, og 5G-oppkoblinger står for om lag 5 % av den totale internettrafikken. Trafikken for 5G øker i takt med mobiltilbydernes 5G-utrulling og innfasing av nye håndsett som er klargjort for 5G-teknologi.

Internettrafikk i fastnettene

Også i fastnettene vært en årlig vekst i internettrafikk på ca. 25-30 % siden 2017. I første kvartal 2022 var trafikkproduksjonen i nettene hos de største fastnettilbyderne over 2 Tbit/s i travel time (peak hour).

Tilbyderne erfarte en betydelig økning og en endring i trafikkmønsteret i forbindelse med korona-nedstengningen i 2020 og den påfølgende økningen i hjemmekontor og videomøter.

Applikasjonene som produserer mest internettrafikk

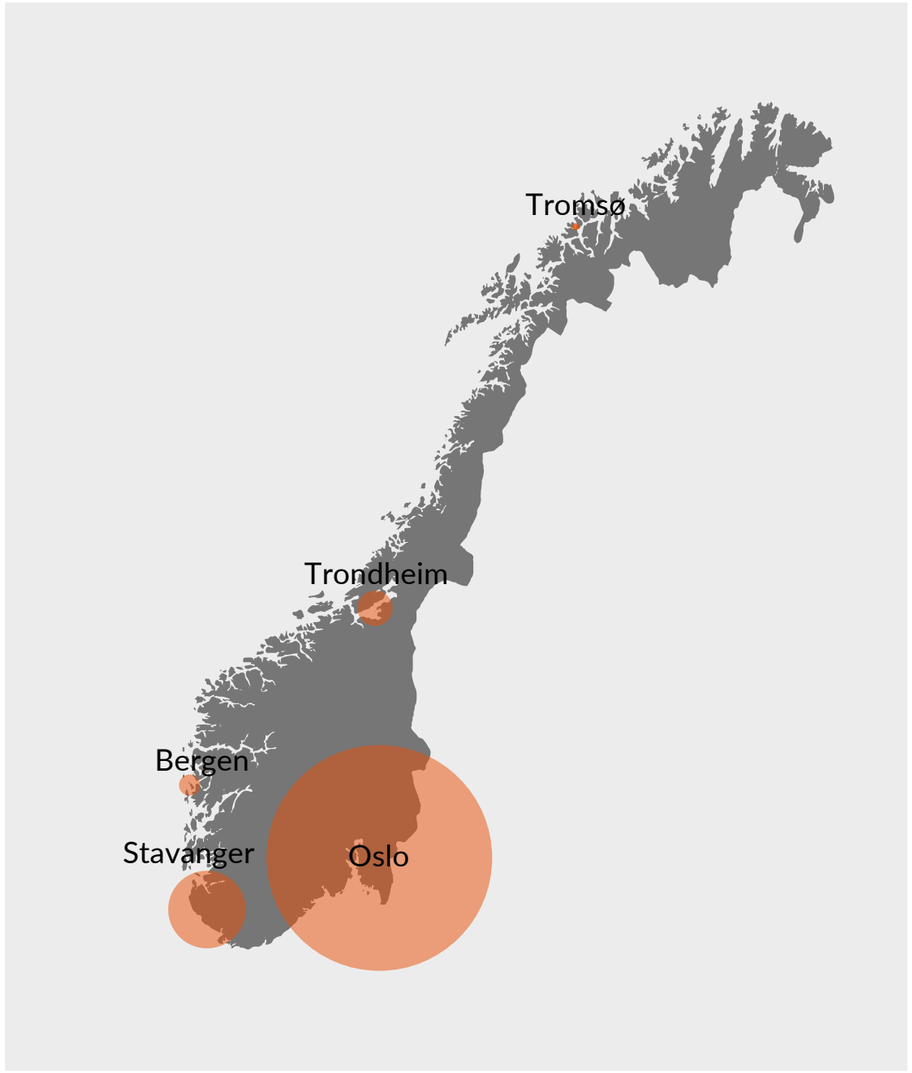
Fordelingen av internettrafikken mellom ulike applikasjoner er relativt lik i mobilnettene og fastnettene. Nettsurfing (HTTP-basert kommunikasjon) er fortsatt den største trafikkdriveren. Strømmetjenester som nett-TV, YouTube, Netflix og TikTok, er en stor bidragsyter. Deretter følger sosiale medier som Facebook, Instagram og Snapchat.

Trafikkutvikling på NIX

Som nevnt i kapittel 2.2. skjer samtrafikken mellom de ulike norske nettene og samtrafikken mellom norske og utenlandske nett, hovedsakelig i Oslo. En del av den norske samtrafikken skjer på de offentlige samtrafikkpunktene NIX. Figur 8 viser plasseringen av samtrafikkpunktene, og boblenes størrelse illustrerer den relative forskjellen i trafikkmengde i 2021.

Årsgjennomsnitt for innkommende/utgående internettrafikk i hele NIX-infrastrukturen er 102 Gbit/s i 2021[16], hvor NIX1 og NIX2 i Oslo utgjør 96 Gbit/s (94 % av den totale trafikken på NIX).

16 | Statistics – nix.no, dataene ble innhentet i april.2022.



Figur 8 - Lokalisering og trafikkvolum for samtrafikkpunktene til NIX

Gitt at også det meste av privat samtrafikk skjer i Oslo, er det tydelig at det i Norge er svært liten grad av regional samtrafikk. Ett unntak synes å være Stavanger (SIX) som har hatt størst økning i 2021, med årsgjennomsnitt på 5 Gbit/s. SIX er plassert i datasenteret Green Mountain, og veksten skyldes nye innholdstilbydere og tilbydere av CDN (Content Delivery Network), samt at antall tilkoblede nett har økt.

2.3 Utbredelse av IPv6

I 2022 har Norge en IPv6-utbredelse på 22,2 %, og rangerer med dette på 35. plass i verden. I oktober 2020, var Norge på 29. plass med utbredelsen 18,1 %. Norge har altså falt 6 plasser på listen i løpet av 1½ år. Samtidig har prosentandel for IPv6-utbredelse forbedret seg og økt med ca. 4 prosentpoeng. På europeisk nivå ligger Norge på 14. plass.

Dette vil si at internettaktørene i en del andre land øker IPv6-utbredelsen raskere enn det norske markedet. Nkom følger utviklingen videre og understreker viktigheten av at aktørene i det norske markedet legger til rette for bruk av IPv6 i størst mulig grad.

2.3.1 Om overgangen fra IPv4 til IPv6

Regjeringens mål er «*At Nasjonal kommunikasjonsmyndighet i samarbeid med relevante parter skal forsere arbeidet med bruk av IPv6, slik at Norge minst er på høyde med sammenlignbare land*». Nkom vil på denne bakgrunn søke å kartlegge dagens status for bruk av IPv6 i Norge, samt å følge utviklingen over tid.

IP (Internet Protocol) er den grunnleggende protokollen som brukes for å overføre trafikk på internett, samt å identifisere enhetene koblet til internett (datamaskiner, telefoner, servere etc.). Offentlige IP-adresser er unike verdensomspennende identifikatorer. IP-protokollen finnes i to versjoner, IPv4 og IPv6.

IPv4 har vært brukt på Internett siden 1983. Internetts suksess, kombinert med mangfoldet av bruksområder og det voksende antall tilkoblede enheter, har resultert i en gradvis nedgang i antall ledige IPv4-adresser, der enkelte deler av verden er hardere rammet av den sterkt reduserte tilgjengeligheten enn andre.

Den grunnleggende IPv6-spesifikasjonen ble ferdigstilt i 1998, og i årene etter har de vært utført et omfattende standardiseringsarbeid for protokollen. IPv6 tilbyr et svært høyt antall IP-adresser, som antas å være tilstrekkelig i lang tid fremover. I tillegg gir protokollen funksjoner for økt grunnleggende sikkerhet og optimalisert ruting.

Kompleksiteten til dagens Internett medfører at overgangen fra IPv4 til IPv6 må gjøres gradvis. Det er nødvendig med en lengre periode av sameksistens mellom de to versjonene. Først når alle internettilknyttede enheter har migrert til ny versjon, vil IPv6 fullt ut kunne erstatte IPv4. Selv om overgangen begynte i 2003, er prosessen fortsatt i en fase av sameksistens.

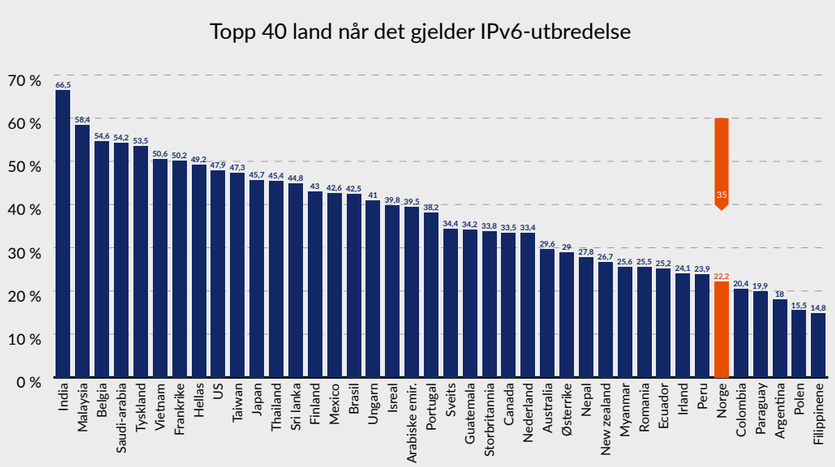
25. november 2019 kunngjorde RIPE NCC[17] at de hadde gått tom for IPv4-adresser. Dette vil kunne medføre akselerasjon i overgangen fra IPv4 til IPv6.

17 | RIPE NCC - det regionale Internett-registeret som har i oppgave å tildele IP-adresser i Europa og Midtøsten

2.3.2 IPv6-utbredelsen i Norge

Figur 9 nedenfor viser status for IPv6-utbredelsen i Norge. Datagrunnlaget er hentet fra de fire hovedkildene med offentlig tilgjengelig informasjon rundt IPv6-utbredelse (Google, Akamai, Facebook, Apnic)[18]. Datainnsamlingen ble utført i april 2022. Denne første årsrapporten for *Internett i Norge* er ment som et utgangspunkt for å observere utviklingen av IPv6-utbredelsen. Norge rangerer på 35. plass på verdensbasis med en utbredelse på 22,2 %. På europeisk nivå ligger Norge på 14. plass.

Basert på informasjon fra Frankrikes internettrapport[19] for 2021, hvor dataene er fra oktober 2020, var Norge på 29. plass med en IPv6-utbredelse på 18,1 %. Norge har falt tilbake 6 plasser på listen for topp land når det gjelder IPv6-utbredelse i løpet av 1½ år (fra oktober 2020 til april 2022), men prosentandelen for IPv6-utbredelse har likevel forbedret seg i perioden, og økt med ca. 4 prosentpoeng (fra 18,1 % til 22,2 %). På europeisk nivå var Norge på 12. plass på det tilsvarende tidspunktet (oktober 2020), det vil si at Norge her har falt to plasser på listen i løpet av 1½ år.



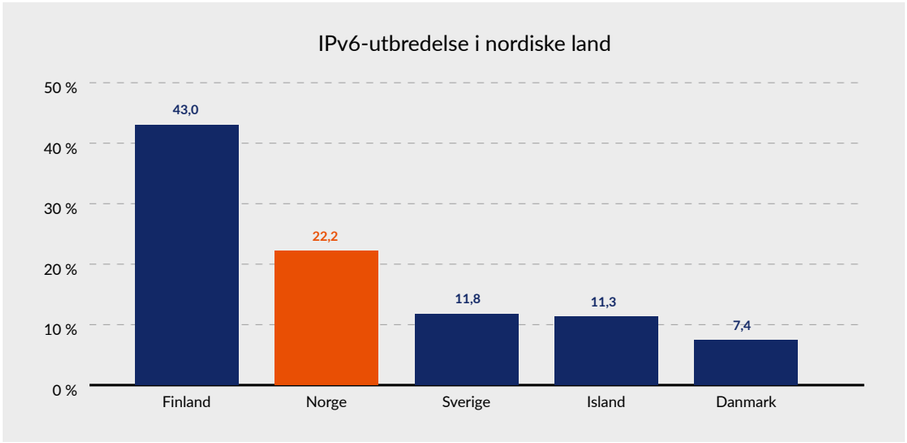
Figur 9 - Topp 40 land når det gjelder IPv6-utbredelse

Til tross for at Norge har falt noe bakover på listen, har IPv6-utbredelsen økt gradvis hos de norske internettilbyderne. At IPv6-utbredelsen øker nasjonalt mens Norges posisjon i listen flytter seg nedover, betyr at internettilbydere i mange land akselererer IPv6-utbredelsen raskere enn internettilbydere i det norske markedet.

18 | Basert på medianen for «Google IPv6-utbredelse», «Akamai IPv6-utbredelse», «Facebook IPv6-utbredelse», «Apnic IPv6-utbredelse», -data fra april 2022. Medianen av de fem kildene er beregnet for hvert land, statistikken gjelder bare de 100 landene med flest internettbrukere (kilde: Wikipedia, data per april.2022).

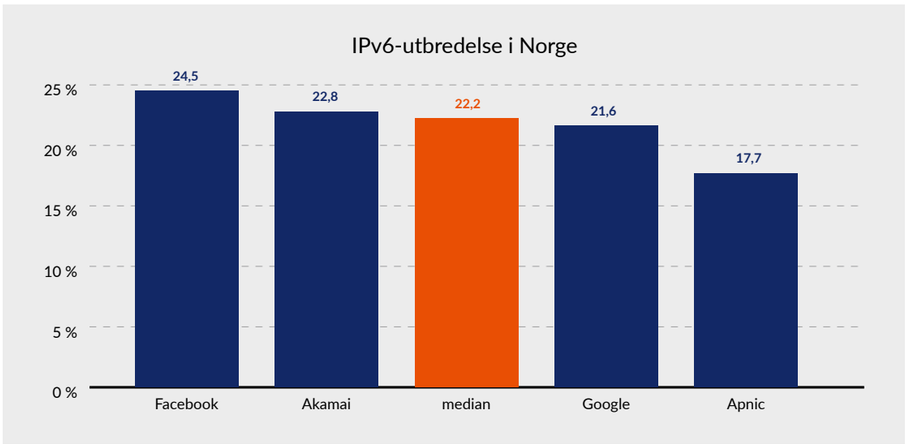
19 | The state of the internet in France – en.arcep.fr, 2021 edition

Figur 10 viser hvordan Norge er plassert blant de nordiske land når det gjelder bruk av IPv6. Norge er på andreplass, bak Finland og foran Sverige, Island og Danmark.



Figur 10 - IPv6-utbredelse i nordiske land

Figur 11 viser utbredelsen i prosent medianverdi hentet fra de fire hovedkildene til offentlig tilgjengelig informasjon om IPv6-utbredelse (Google, Akamai, Facebook, Apnic). Facebook registrerer den høyeste IPv6-utbredelsen i prosent blant norske sluttbrukere.



Figur 11 - IPv6-utbredelse i Norge

2.3.3 Status for norske internettilbyderne

Nkoms informasjonsinnsamling viser at det utelukkende er «dual stack» som tilbys de norske kundene. Det vil si at IPv4 og IPv6 kjøres parallelt i både fast- og mobilnettenes infrastruktur. Brukerne hos de aller fleste fast- og mobilnettilbydere må selv ta initiativ («opt-in») for å ta i bruk IPv6, gjennom å aktivere IPv6 på sine rutere og/eller gjennom omkonfigurering av sin terminal.

Når det gjelder internett*samtrafikk*, ser det ut til at IPv6 har en langt større utbredelse. Alle de spurte fast- og mobilnettilbyderne benytter IPv6, så sant samtrafikkpartnerne også støtter dette. Når det gjelder ruting av trafikk, stabilitet, sikkerhetsnivå og ytelse for spesielt spilltjenester, rapporteres det ikke om noen opplevd forskjell mellom IPv4 og IPv6.

IPv6 i mobilnettene

To av tre mobiltilbydere tilbyr IPv6 i sine nett, mens den tredje vil få dette på plass i nær fremtid. En stor del av taletrafikken (VoLTE) går over IPv6, avhengig av om håndsettene støtter dette eller ikke. Internettrafikk i mobilnettene (inkludert fast trådløst bredbånd) benytter per i dag IPv6 i liten grad.

Mobiltilbyderne tilstreber at de mest brukte terminalene er forhåndskonfigurert til å støtte IPv6, og at det ved «dual stack» er IPv6 som foretrekkes.

IPv6 i fastnettene

Noen fastnettilbydere har støtte for IPv6 aktivert for alle nye leveranser, mens andre tilbydere forespør kundene om de ønsker dette. Noen av tilbyderne kan aktivere/deaktivere IPv6 fullt ut fra sin side, mens det i andre tilfeller også kreves at kunden konfigurerer kundeutstyret selv. Dette er oftest bestemt av hvorvidt kunden benytter utstyr levert av tilbyder eller anskaffer utstyr selv.

Fastnettilbydere har i liten grad oversikt over IPv6-bruken. Blant privatkunder er det i all hovedsak de «spesielt interesserte» som velger IPv6. I det offentlige og bedriftsmarkedet er det noe mer bruk av IPv6. Fastnettilbydere må også gi noen kunder nytt utstyr dersom IPv6 skal benyttes. Tilbakemeldingene tyder på at IPv6 i liten grad «selges inn», på tross av at infrastrukturen som sådan ofte er forberedt for IPv6.

2.4 Domenenavnsystemet

Det er nylig tatt i bruk nye metoder for domeneoppslag, såkalt «kryptert DNS». Én av disse metodene er DoH (DNS-over-HTTPS). Dagens tilbydere av DoH-oppslagstjenere ligger i hovedsak utenfor norsk jurisdiksjon. Det foreligger flere regulatoriske konsekvenser ved økende bruk av åpne oppslagstjenere, blant annet at myndighetsutøvelse basert på filtrering av DNS-oppslag håndheves i mindre grad.

EU har iverksatt initiativet DNS4EU som skal etablere et europeisk alternativ til de store amerikanske åpne DNS-oppslagstjenerne. Nkom vil fremover følge utviklingen av DNS4EU etter hvert som løsningen blir tilgjengelig og vurdere muligheten for norsk involvering og tilrettelegging for bruk av tjenesten for norske borgere. En slik tilnærming vil på sikt kunne bidra til å styrke posisjonen til DNS-oppslagstjenere innen europeisk jurisdiksjon.

2.4.1 Status DNS i Norge

Domenenavnsystemet (DNS) knytter IP-adresser til unike domenenavn, som altinn.no. Dette er en grunnleggende funksjon som er nødvendig for at internettinfrastrukturen skal fungere. Når en bruker forsøker å kontakte en tjeneste på internett utløser det en rekke oppslag i DNS for å finne den aktuelle IP-adressen. Den hierarkiske oppbygningen til systemet krever et samspill fra flere uavhengige aktører for at brukerens maskin skal få det svaret den trenger.[20]

Norid AS er registerenheten for de norske landkodetoppdomenene .no, .sj og .bv, og har i henhold til overenskomst med den internasjonale forvalter av toppdomener (ICANN) rett til å tildele, administrere og registrere domenenavn under disse toppdomenene. Det er kun .no-domenet som er åpent for registreringer. Som registerenhet forvalter Norid navnetjenesten og registreringstjenesten for toppdomenene.

Et domenenavn oppstår i det en organisasjon eller privatperson får tildelt et abonnement på domenenavnet. Norids registreringstjeneste behandler søknader om domenenavn i tråd med gjeldende tildelingsregler og opprettholder register over bruksrett til de ulike domenenavnene. For å søke om et domenenavn må en søker kontakte en domeneforhandler, som sender inn søknaden og deretter administrerer abonnementet på abonnentens vegne. Det er rundt 260 forhandlere som videreformidler domenenavn som slutter på .no.

Navnetjenesten til .no er en del av den tekniske infrastrukturen til domenenavnsystemet. Tjenesten svarer på hvilke domenenavn som finnes under toppdomenet og hvilke navnetjenere hvert enkelt domenenavn er knyttet til. Den har særlig høye krav til tilgjengelighet, og har ikke vært utilgjengelig siden toppdomenet ble tatt i bruk for over 30 år siden.

I 2014 introduserte Norid DNSSEC for norske domenenavn. DNSSEC er en sikkerhetsmekanisme som kryptografisk signerer svar på domeneoppslag. Dette gjør det mulig å kontrollere at svar på oppslag i DNS kommer fra riktig kilde, og ikke er endret underveis. Per mai 2022 er 60,8 % av alle domenenavn under .no signert med DNSSEC, og det norske toppdomenet ligger i verdenstoppen i andelen sikrede domenenavn.

Selv om .no har en svært høy andel sikrede domenenavn totalt, er det store forskjeller på graden av sikring hos de ulike domeneforhandlerne. Fem av de ti største domeneforhandlerne har signert mer enn 80 % av domenenavnene de forvalter. De øvrige har signert mindre enn 5 % av porteføljene sine, eller tilbyr ikke slik sikring av kundenes domenenavn.

En forutsetning for at DNSSEC kan sikre den enkelte bruker er at maskinen som henter svaret på domeneoppslaget, sjekker (validerer) svaret slik at svar med falske eller mangelfulle signaturer forkastes. Dette gjøres av spesielle maskiner – oppslagstjenere – som ofte drives av internettilbydere, lagringstilbydere og tjenesteansvarlige i bedriftsinterne nett.

Per mai 2022 valideres om lag 86,2 % av domeneoppslagene i Norge, noe som også på verdensbasis er høyt. Det skyldes blant annet at store aktører som Telenor, Telia og Altibox, som til sammen dekker en stor kundemasse, har slått på validering. Det er imidlertid fortsatt enkelte store internettilbydere som ikke validerer domeneoppslagene.

20 | Delkapittel 2.4.1 er et tekstbidrag fra Norid

2.4.2 Krypterte domeneoppslag

Hva er «kryptert DNS»?

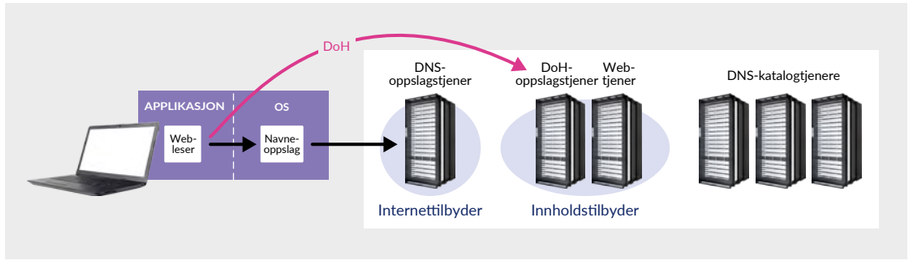
Domenenavnsystemet består av to hoveddeler:

- katalogtjenere, såkalte autoritative DNS-tjenere som inneholder den globale katalogen av domenenavn, og
- oppslagstjenere, såkalte rekursive DNS-tjenere (DNS-resolvere) som utfører oppslag i denne katalogen.

Når vi kommuniserer over internett og skriver inn en domeneadresse, sender datamaskinen vår først en forespørsel om navneoppslag til en oppslagstjener som typisk tilbys av internettilbyderen vår. Oppslagstjeneren spør deretter katalogtjenerne på internett for å finne den aktuelle IP-adressen og returnere denne til vår datamaskin.

I dag er det også blitt vanlig at andre aktører enn internettilbyderne tilbyr oppslagstjenere, som ulike innholdstilbydere som også tilbyr «åpne» oppslagstjenere. Det vil si at vi kan konfigurere webleseren vår til å benytte disse oppslagstjenerne i stedet.

Relativt nylig er nye metoder for navneoppslag tatt i bruk, såkalt «kryptert DNS». Én av disse metodene er DoH (DNS-over-HTTPS) som utfører navneoppslag som en integrert delt av webtrafikken. Dagens tilbydere av DoH-tjenere ligger hovedsakelig utenfor norsk jurisdiksjon.



Figur 12 - Domeneoppslag med henholdsvis tradisjonell DNS og DoH

Bruken av DoH får ulike konsekvenser for ulike kategorier aktører. For vanlige internettbrukere byr kryptering på fordeler i form av konfidensialitet for navneoppslagene man gjør. Organisasjonen som driver oppslagstjenesten vil imidlertid ha tilgang til oppslagene som gjøres, og da er spørsmålet om man stoler mest på en nasjonal internettilbyder eller en internasjonal innholdstilbyder.

Betydningen av disse forholdene avhenger også av hvor man bor eller oppholder seg, samt hvem man er. For eksempel for dissidenter i et autoritært land vil vurderingene typisk være annerledes enn for norske borgere. Innføring av kryptert DNS har også ulike konsekvenser for andre aktører som belyses nærmere i de følgende delkapitlene.

Den detaljerte virkemåten til kryptert DNS er fortsatt under utvikling. Selve den grunnleggende protokollen er ferdig standardisert. Det arbeides fortsatt med å forbedre funksjonaliteten for å konfigurere hvilken DoH-tjener som benyttes av webleseren. Når dette kommer på plass, vil mulighetene for å sette opp kryptert DNS på ønsket måte bli vesentlig bedre.

Status DNS-over-HTTPS (DoH)

DOH støttes i økende grad av de mest populære weblesere og operativsystem. Eksempelvis støttes DoH av webleserne Firefox, Chrome og Edge, og kan også finnes i operativsystem som Windows, MacOSX og Linux samt Android og iOS.

Standardisering av mekanismer knyttet til policy for valg av oppslagstjenere drives av IETF i arbeidsgruppen «Adaptive DNS Discovery». Inntil videre er valg av oppslagstjener implementasjonsspesifikk og varierer mellom både weblesere og operativsystem.

For flere av implementasjonene er DoH imidlertid ikke påskrudd som standard operasjonsmodus. Det er all grunn til å tro at dette er en utvikling som vil endre seg, og vil implementeres gjennom en rask oppdatering. Eksempelvis ble det i 2021 skrudd på DoH som standard for alle brukere av Firefox i Nord-Amerika.[21]

Åpne oppslagstjenere har lenge vært tilgjengelig for internettbrukerne. Flere av tilbyderne av slike har også i løpet av de siste årene implementert mulighet for å benytte DoH. For norske forbrukere er det valgfritt hvilken oppslagstjeneste en benytter, dette på tross av at slik bruk fjerner kontroll på kundeopplevelse fra internettilbyderne. Norske internettilbydere tilbyr til dags dato ikke DoH som mekanisme fritt tilgjengelig for sine kunder.

DoH setter som mål å sikre kommunikasjonen mellom internettbruker og tilbyder av oppslagstjenesten. Norske forbrukere er i stor grad beskyttet mot innsyn i deres bruk av DNS gjennom lovgivning, og det foreligger stor tillit mellom kunder og internettilbydere. Dette fører til et begrenset insentiv for å endre dagens oppslagstjenester. Videre foreligger det en del tekniske utfordringer ved bruk av DoH knyttet til responstid, skalering og tilgang på og erfaring med implementasjoner av DoH-tjenere.

2.4.3 Regulatoriske konsekvenser av DoH

Regjeringens mål er å «*Arbeide for at norske internettilbydere skal opprettholde oppslagstjenere innenfor norsk jurisdiksjon ved innføring av nye metoder for navneoppslag*».

Det foreligger flere regulatoriske konsekvenser ved bruk av åpne DNS-oppslagstjenere generelt og åpne DOH-oppslagstjenester spesielt, siden myndighetsutøvelse basert på begrensninger i DNS ikke lenger lar seg gjennomføre regulatorisk.

Lovpålagt tilretteleggingsplikt etter ekomloven, eksempelvis knyttet til avlytting, vanskeliggjøres ved bruk av DoH der trafikken i sin helhet er kryptert. Videre er det ikke mulig å skille domeneoppslag fra annen internettrafikk. Dette fører til at det er vanskelig å avgjøre hvorvidt det brukes DoH, samt å kunne detektere innhold i forespørsler og svar.

DNS brukes også for nasjonalt pålagt filtrering, eksempelvis basert på Pirate Bay-dommen. I de tilfellene hvor det benyttes åpne oppslagstjenere med DoH, forsvinner muligheten til å filtrere vekk ulovlig innhold. Flere av de populære åpne oppslagstjenerne drives av større multinasjonale selskap hvor det er vanskelig å utøve norsk myndighet.

Ytterligere ansvarsforhold i henhold til ekomlovens pålegg om sikker og forsvarlig drift vil også kunne brytes opp med DoH. Internettilgangstjenesten er i stor gradavhengig av kontroll og stabilitet i DNS. Ved bruk av internasjonale oppslagstjenester mister internettilbyderne deler av denne kontrollen.

21 | Firefox extends privacy and security of Canadian internet users with by-default DNS-over-HTTPS rollout in Canada

I forbindelse med den økende bruken av åpne oppslagstjenester fra amerikanske aktører som Google og Cloudflare, har EU iverksatt initiativet DNS4EU som et europeisk alternativ. Ved idriftsettelse av DNS4EU vil tjenesten gi et valgfritt tilbud som supplerer eksisterende oppslagstjenester, og som støtter oppdaterte sikkerhetskrav og personvern etter europeisk standard, inkludert støtte for filtrering basert på nasjonale domsavgjørelser.

Nkom vil fremover følge utviklingen av DNS4EU etter hvert som løsningen blir tilgjengelig og vurdere muligheten for norsk involvering og tilrettelegging for bruk av tjenesten for norske borgere. En slik tilnærming vil på sikt kunne bidra til å styrke posisjonen til DNS-oppslagstjenere innen europeisk jurisdiksjon.

2.5 Tingenes internett

Antall IoT-enheter øker i både lisensierte og ulisensierte frekvensbånd. I 2023 vil utbyggingen av frittstående 5G starte og vil sannsynligvis på sikt overta store deler av IoT-trafikken. Fra 1. august 2024 vil Europakommisjonens regulering om internettsikkerhet for IoT-utstyr være gjeldende for produsenter av radioutstyr.

Det er fortsatt mye IoT-utstyr i Norge som kun er koblet til 2G-nett. 2G-nettene planlegges imidlertid nedlagt i 2025. Nkom oppfordrer alle bransjer til å starte planlegging av utfasing av enheter som kun virker på 2G. Nkom vil også kartlegge bruk og avhengigheter av 2G, og eventuelle utfordringer som oppstår i tiden frem mot slukkingen av 2G-nettet, for å sikre en forsvarlig avvikling som ivaretar relevante brukerhensyn.

2.5.1 Anvendelse av tingenes internett

Tingenes internett (Internet of Things, IoT) består av fysiske gjenstander som kommuniserer direkte eller indirekte via internett. Kommunikasjon mellom IoT-enheter uten menneskelig interaksjon omtales som maskin-til-maskin (M2M) kommunikasjon. Avhengig av datamengde, kommunikasjonsmønster, krav til rekkevidde, strømforbruk, bevegelighet og antall enheter vil det brukes ulike teknologier.

IoT-enheter kan tilkobles via trådbasert eller trådløs tilknytning. For trådløs tilknytning går det et hovedskille mellom teknologier som benytter frekvenser regulert av fribruksforskriften (ulisensierte frekvenser) og teknologier som bruker mobilteknologi (lisensierte frekvenser).

Antall IoT-enheter har økt kraftig de senere årene og trenden ser ut til å fortsette. Tall fra analyseselskapet IoT Analytics anslår at det var om lag 12 milliarder IoT-enheter i verden i 2020[22]. Dette anslås å stige til 31 milliarder i 2025.

I Norge benyttes IoT innen en rekke områder, som alarmsystemer, betalingsløsninger, smarthussystemer og målesystemer, f.eks. strømmåling. Innen transportsektoren benyttes IoT for alarmering, styring og sporing av kjøretøy og containere samt for elektronisk kjørebok. Innen helsesektoren er det anvendelser som trygghetsalarmer i hjemmene og pasientvarsling på sykehjem. Trenden er også at en rekke tradisjonelle husholdningsprodukter som kjøleskap, vaskemaskiner, tørketromler, kaffetraktere og liknende blir IoT-produkter.

22 | State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time

2.5.2 IoT som ekomtjeneste

IoT via ulisensierte frekvenser

I denne kategorien finner vi en rekke protokoller med forskjellig rekkevidde og båndbredde. De mest kjente er Wi-Fi, Bluetooth/BLE (Bluetooth Low Energy), ZigBee, Z-wave, LoRaWAN og Sigfox. De to siste går under fellesbetegnelsen LPWAN (Low-Power Wide-Area Network).

Utviklingen i bruk av ulisensierte frekvenser er økende, og antall tilkoblede enheter stiger sterkt. Det er imidlertid vanskelig å estimere denne utviklingen nøyaktig siden mye utstyr ikke behøver å registreres. Selskapet Last Mile Solutions rapporterer om svært høy vekst de foregående tre årene og forventer også sterk vekst de nest tre årene.

En av de mest brukte trådløse IoT-protokollene er LoRaWAN som med god dekning og lavt strømforbruk har store bruksområder. Teknologien kan for eksempel benyttes i vannmålere, bevegelsessensorer og temperatursensorer. For ulisensierte teknologier med begrenset rekkevidde kan det være nødvendig å supplere med lisensiert nett, som 4G/5G.

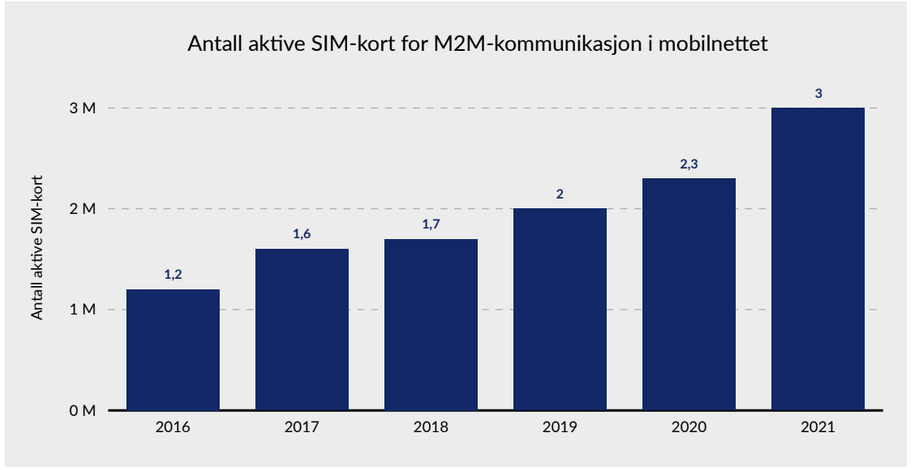
IoT via lisensierte frekvenser

2G (GSM) ble opprinnelig utviklet for kommunikasjon mellom mennesker og ikke som bærer for IoT. SMS ble imidlertid tatt i bruk til enkel IoT-kommunikasjon og er fortsatt i utbredt bruk. 2G-nettene har begrensninger både når det gjelder overføringskapasitet og antall tilkoblede enheter.

I 4G (LTE) ble to IoT-spesialiserte standarder introdusert: LTE-M og NB-IoT. LTE-M gir mulighet for høyere hastighet og mobilitet enn NB-IoT. NB-IoT er en enklere protokoll med lavere strømforbruk som er godt egnet for hyppig kommunikasjon og god dekning innendørs. Dette har gitt økende interesse for og bruk av mobil-IoT fra næringsliv og industri.

De siste to årene har mobiltilbyderne bygd ut 5G-nett i Norge. 5G støtter et stort antall samtidig tilkoblede enheter i nettet med mulighet for å håndtere flere bruksområder. Dagens 5G-nett har ikke støtte for dedikert M2M-teknologi, men dette er forventet å bli tilgjengelig med innføring av frittstående 5G (5G Stand Alone) og skivedeling som kommer i løpet av 2023.

Figur 13 viser antall aktive SIM-kort for M2M i mobilnettene i Norge. Statistikken viser at antall aktive SIM-kort i 2021 er nær doblet siden 2017 og at antall enheter stiger raskere for hvert år.



Figur 13 - Antall aktive SIM-kort for M2M-kommunikasjon i mobilnettet

I dag benytter mobiltilbyderne både 2G og 4G for M2M-kommunikasjon, men de planlegger å stenge 2G-nettene i løpet av 2025. Dette vil få betydelige konsekvenser for bransjer som fortsatt kun benytter 2G til M2M. Det er fortsatt over en million IoT-enheter koblet til 2G-nett.

Nkom oppfordret alle bransjer til å starte planlegging av utfasing av enheter som kun virker på 2G frem mot tidspunktet for tilbydernes planlagte slukking av 2G-nettet[23]. I tiden frem mot slukketidspunktet vil Nkom fortsette kartleggingen av bruk og avhengighet av 2G, for å sikre en forsvarlig avvikling som ivaretar relevante brukerhensyn.

2.5.3 IoT-sikkerhet

IoT-enheter kan utnyttes til dataangrep og spredning av ondartet programvare. Enhetene kan også selv være mål for dataangrep som manipulerer virkemåte eller stjeler persondata. Det foreligger i dag ikke krav til at IoT-utstyr skal ha innebygget beskyttelse, og ansvaret for å beskytte seg mot slike hendelser er i dag hovedsakelig overlatt til brukerne selv.

Europakommisjonen har konkludert med at dette er et så stort problem at EU etablerer egen regulering på området[24]. Kravene vil gjelde internettilkoblet radioutstyr og krever innebygd datasikkerhet, personvern, beskyttelse mot svindel og beskyttelse av nettet. Reguleringen gjelder for utstyr plassert på markedet etter 1. august 2024.

Europeiske standardiseringsorganisasjoner arbeider med å ta fram relevante harmoniserte standarder på området. For IoT-utstyr beregnet til forbrukere er det allerede utarbeidet en standard (EN 303 645) som beskriver god praksis for beskyttelse av data og personvern. Standarden er rettet mot utviklere og produsenter av IoT-utstyr.

2.6 Internettsikkerhet

Pressen har ofte søkelys på sikkerheten i sluttbrukerutstyr, som datamaskiner, mobiltelefoner, nettbrett og lignende. For enkeltpersoner kan dårlig sikkerhet og vellykkede dataangrep medføre store konsekvenser.

Trusselaktørene utnytter imidlertid også internetts kjernefunksjoner som DNS og BGP. Nettene utsettes ofte for distribuerte tjenestenektangrep. Fellesnevneren er at sluttbrukerne er avhengige av tilbyderne for tiltak mot denne formen for sikkerhetsangrep.

2.6.1 Om internettsikkerhet

Kompleksiteten i internetteknologien øker, og verdikjedene blir lengre og mer uoversiktlige. Når dette kombineres med økende antall sårbarheter i infrastruktur og tjenester, samt flere ondsinnede trusselaktører, stilles det sterke krav til internettilbyderne for å bidra til sikre og stabile tjenester.

Grunnleggende funksjoner på internett er under press for utnyttelse. Protokollene blir imidlertid kontinuerlig oppdatert med nye sikkerhetsfunksjoner for å møte de ulike trusler. Norge ligger langt framme i å ta i bruk slike sikkerhetsforbedringer.

23 | Informasjon om slukking av 2G-nett i 2025 – nkom.no

24 | Nye krav styrker sikkerheten i radioutstyr – nkom.no

2.6.2 Sikkerhet for internetts kjernefunksjoner

Domenenavnsystemet

DNS er en kritisk kjernefunksjon på internett som er utsatt for sikkerhetsangrep. Kapring og manipulering av DNS kan føre til at brukere blir rutet til falske nettsteder. Disse iboende sårbarhetene er knyttet til både drift og bruk av DNS-infrastrukturen.

Historisk er det observert større sårbarheter både i DNS-protokollen og i implementasjoner av denne. DNS-protokollen har i flere tilfeller blitt benyttet til distribuerte tjenestenektangrep (DDoS) som utnyttet grunnleggende funksjonalitet i DNS og måten delegering og videresending av forespørsler fungerer.[25]

Drift av autoritative navnetjenere er distribuert og gjøres av eierne av domenene. Dette fører til at et stort antall aktører må sikre sine systemer, som i varierende grad klarer å gjennomføre dette. Det finnes ulike tekniske løsninger som kan sikre domeneoppslagene, men disse tas ikke alltid i bruk. For norske domener er tilstanden relativt god på dette området, hvor om lag 60% av domenene er signert basert på DNSSEC, jf. kapittel 4.1.

Selv om DNSSEC benyttes til å sikre at svar på navneoppslagene ikke manipuleres av uvedkommende, sikrer ikke dette at eierskap til forespurt domene er riktig. Trusselaktører kan utnytte dette ved å registrere domener som ligger nært i stavemåte eller registreres på alternative toppdomener. Mulighet for å registrere denne type falske domener er avhengig av policy og sikringstiltak ved registrering i de ulike toppdomene. Eksempelvis har Norid strenge retningslinjer som ivaretar merkevare og egennavn under .no sonen, mens dette i mindre grad utføres for generiske toppdomener som er internasjonalt tilgjengelig. Nkom EkomCERT rapporterer ukentlig på hendelser knyttet til falske domener.

Border Gateway Protocol

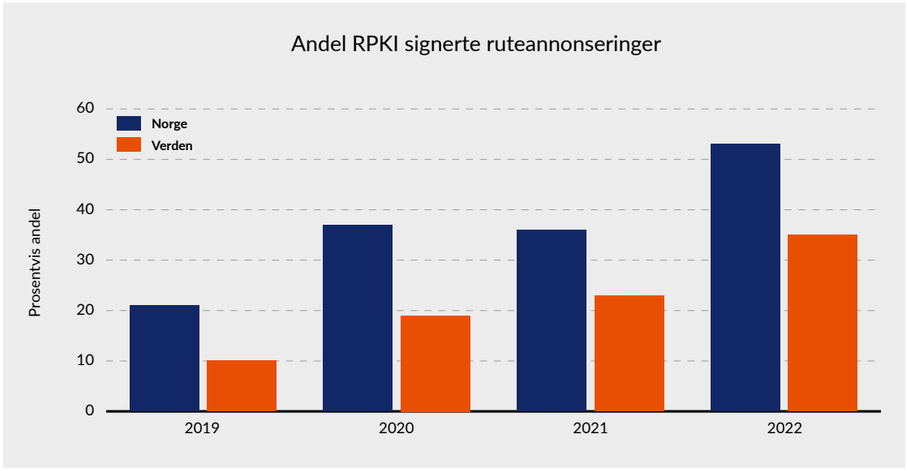
Border Gateway Protocol (BGP) er rutingprotokollen som benyttes for å binde sammen nettene (autonome system) til et globalt internett. BGP lar de ulike internettilbyderne annonsere hvilke adressesegment som benyttes i deres nett, og derved kan de ulike ruterne på internett lære den korteste veien til andres nett og adresser.

Det finnes tekniske løsninger for å verifisere eierskap og sikre ruteannonseringer via BGP. En metode som benyttes er Resource Public Key Infrastructure (RPKI) som kryptografisk bekrefter eierskap via esignatur. Norske nett er i voksende grad beskyttet av denne type signeringer, men har fremdeles et stykke igjen. Verifisering utføres også i større grad, hvor det benyttes Routing Policy Specification Language (RPSL).

Det jobbes også med utvikling og standardisering av tilsvarende sikringsmekanismer for hele nettverkstier som annonseres via BGP. Dette arbeidet er imidlertid ikke modent nok til at det er i utstrakt bruk. De siste årene har flere større netteiere signalisert at annonsering må sikres med RPSL og/eller RPKI og kunne valideres for at ruteannonseringer skal bli akseptert.[26]

25 | Eksempler på slike sårbarheter er tsuNAME og NXNSAttack.

26 | Is BGP safe yet? No.



Figur 14 - Andel signerte ruteannonseringer, kilde: https://observatory.manrs.org/#/overview

En angrepsmetode som benytter BGP er såkalt BGP-kapring, som innebærer at en aktør annonserer adressesegment de ikke rettmessig opererer, noe som fører til at internettrafikk rutes til eller via feil nett. Konsekvensene av BGP-kapring er potensielt meget store, blant annet kan en trusselaktør utføre tjenestenektangrep, avlytte trafikk eller introdusere forfalsket infrastruktur og tjenester.

BGP-kapring kan også forekomme utilsiktet som en følge av feilkonfigurasjon av nettverksutstyr og BGP-ruting. Ved utbruddet av krigen i Ukraina var det flere observasjoner av BGP-kapring av ukrainske ruteannonseringer.

2.6.3 Tjenestenektangrep og tilgjengelig båndbredde

Tjenestenektangrep er en vedvarende type sikkerhetsangrep som håndteres av norske internettilbydere på daglig basis. Det finnes flere typer tjenestenektangrep. Den mest vanlige berører internetts infrastruktur ved at overføringskapasiteten i nettet forsøkes overlastet ved overføring av store mengder uønsket trafikk. Angrepene er ofte rettet mot sluttkunder eller sluttkunders tjenester.

Det finnes flere mottiltak som kan benyttes. For at dette skal være effektivt er det viktig å ha oversikt over hvilke tjenester eller kunder som ofte er mål for denne type angrep. Det er også viktig med teknisk informasjon rundt metodene som brukes, samt sårbare tjenester eller botnets som kan benyttes i til slike angrep.

De største internettilbyderne har i dag gode mottiltak som kan benyttes for å håndtere tjenestenektangrep. Eksempelvis gjennom filtrering av uønsket trafikk ved bruk av utstyr som er spesielt utformet og designet for dette. Det er også mulig for tilbyderne å samarbeide om å filtrere vekk deler av trafikken ved hjelp av signalering over BGP.

2.7 Internettbaserte tjenester og plattformer

Økende bruk av internettbaserte tjenester og plattformer utfordrer eksisterende lovverk og fordrer tilpasning av lovverket. Innen EU etableres det i disse dager en pakke med regelverk som blant annet Digital Services Act og Digital Markets Act. Disse er EØS-relevante og vil dermed kunne bli del av norsk lov. Nytt regelverk vil legger premisser for forbrukernes og virksomhetenes bruk av internett.

Reguleringen av internettbaserte tjenester og plattformer forutsetter et tverrsektorielt samarbeid mellom myndighetsorganene. Dette for å sikre effektiv og enhetlig myndighetsutøvelse overfor ressurssterke aktører som spiller en dominerende rolle innen internetts økosystem. Nkom vil ta en aktiv rolle i dette samarbeidet på bakgrunn av vår kompetanse som regulatør av elektroniske kommunikasjonstjenester generelt, og regulering av nettnøytralitet og forhåndsdefinerte markeder spesielt.

2.7.1 Regulatorisk utvikling

De senere årene har internettilgang blitt den mest brukte ekomtjenesten i det norske samfunnet. Videre har tjenester som vi benytter via internett (ofte omtalt som «over-the-top») gradvis tatt over for tradisjonelle ekomtjenester. Store datasystemer som tilbyr omfattende internettbaserte tjenester som sosiale medier eller app-butikker, omtales ofte som «internettbaserte plattformer».

I løpet av våren 2022 har EUs lovgivningsinstitusjoner blitt enige om to nye forordninger som skal henholdsvis bidra til å sikre brukernes rettigheter ved bruk av internettbaserte tjenester (Digital Services Act) og som skal etablere såkalt «forhåndsregulering» av de store internettbaserte plattformene (Digital Markets Act). Disse lovverkene inngår i en større pakke med lovforslag knyttet til reguleringen av internett som er EØS-relevante og vil sannsynligvis også bli del av norsk lov i tiden fremover.

2.7.2 Digital Services Act (DSA)

Formålet med DSA er å modernisere og presisere forpliktelser for tilbydere av internettbaserte tjenester og plattformer. Bakgrunnen er en økning i omfanget av forbrukerskadelige aktiviteter på internett. Gjeldende regelverk anses for å være ineffektivt og ikke tilstrekkelig koordinert mellom medlemsstatene til å håndtere dette problemet.

DSA omfatter alle slags tilbydere av internettbaserte tjenester, ikke bare de store plattformene som nevnt i punktet over. Graden av forpliktelser etter DSA avhenger imidlertid av hvor stor tilbyderen er. Veldig store internettbaserte plattformer vil være underlagt flere krav enn mindre mellomliggende tjenester, som tilbydere av internettilgangstjenester, mellomlagringstjenester, og lagringstjenester.

Tilbyderne som omfattes av DSA blir underlagt en rekke ansvarsregler og aktsomhetsforpliktelser som supplerer og utfyller de generelle bestemmelsene. Mindre aktører kan på nærmere vilkår unntas fra enkelte av ansvarsbestemmelsene i regelverket. Store aktører må imidlertid forholde seg til kumulative forpliktelser knyttet til blant annet transparens, rapportering og risikoanalyse.

Håndhevingen av forpliktelsene i DSA vil skje dels nasjonalt, dels internasjonalt. Hvert land vil oppnevne en eller flere nasjonale koordinatorer («Digital Services Coordinators») som får i oppgave å administrere klager på tilbydere, og samarbeide via et europeisk DSA-råd («European Board for Digital Services»). Europakommisjonen vil føre tilsyn med de største plattformtilbyderne.

Nkom støtter forslaget til DSA og mener at asymmetriske forpliktelser er en riktig tilnærming slik at nye og små/mellomstore tilbydere av internettbaserte tjenester ikke underlegges for stor regulatorisk byrde. Tilsynet med veldig store plattformtilbydere forutsetter involvering av Europakommisjonen, siden dette også kan ha side mot annet internettrelatert regelverk, men samtidig vil nasjonale koordinatorer være viktige bidragsytere for å belyse nasjonale forhold og bidra med faglig ekspertise om internett.

Europakommisjonen, Europaparlamentet og Rådet oppnådde politisk enighet om forslaget til DSA den 22. april 2022. Formell godkjenning i Parlamentet og Rådet forventes i løpet av 2. halvår 2022. Deretter vil DSA tre i kraft 15 måneder etter formell godkjenning, eller fra 1. januar 2024, avhengig av hvilket tidspunkt som inntreffer først. De største tilbyderne kan imidlertid bli underlagt tilsyn 4 måneder etter at de har blitt utpekt etter prosedyren som DSA gir anvisning på. [27]

2.7.3 Digital Markets Act (DMA)

Formålet med DMA er å sikre rettferdig behandling av virksomheter som benytter seg av de største internettbaserte plattformene. Et annet viktig hensyn er å gi sluttbrukere og virksomheter mulighet til å anvende plattformene uten å bli møtt med usaklige betingelser av tilbyderen. Ønsket virkning er at regelverket skal stimulere til konkurranse og innovasjon på internett, slik at forbrukere i det indre markedet kan nyte godt av større og bedre utvalg av tjenester på internett til rimelig priser.

Flere aktører vil reguleres av både DSA og DMA, men det sentrale tilbyderbegrepet i DMA er portvokter («gatekeeper»), det vil si innflytelsesrike, internettbaserte plattformer med mange kunder og økonomisk omsetning av slikt omfang at lovgiver har funnet det nødvendig med regulering. Det er også flere vedtak og domstolsavgjørelser på europeisk nivå som har underbygget reguleringsbehovet.

Portvokterne kan utpekes innen forskjellige forretningsområder som er nærmere definert i regelverket, for eksempel internettbaserte ehandelstjenester, søkemotorer, sosiale medier og videodelingstjenester. Selve utpekingen baserer seg på kvalitative og kvantitative kriterier.

Europakommisjonen vil føre tilsyn med DMA, noe som er viktig med tanke på at portvokterne er svært store og dominerende aktører i markedet. Det skal også opprettes en «Digital Markets Advisory Committee» (DMAC), hvor medlemslandene er representert. Videre vil det opprettes en «High-Level Group» hvor BEREC er representert sammen med andre europeiske organisasjoner. Begge organ vil bistå Kommisjonen i sine tilsynsoppgaver.

Nkom støtter også forslaget til DMA og de underliggende formål med regelverket. Portvoktertilbydere begrenser internetts åpenhet på en lignende måte som tilbydere av internettilgang gjorde før regelverket om nettnøytralitet ble innført. Derfor er det avgjørende med regulering som kan sikre internetts åpenhet på applikasjonslaget.

Europakommisjonen, Europaparlamentet og Rådet oppnådde politisk enighet om forslaget til DMA den 24. mars 2022. Formell godkjenning i Parlamentet og Rådet forventes i løpet av 2.halvår 2022. DMA vil tre i kraft 6 måneder etter at regelverket er vedtatt.

27 | Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment

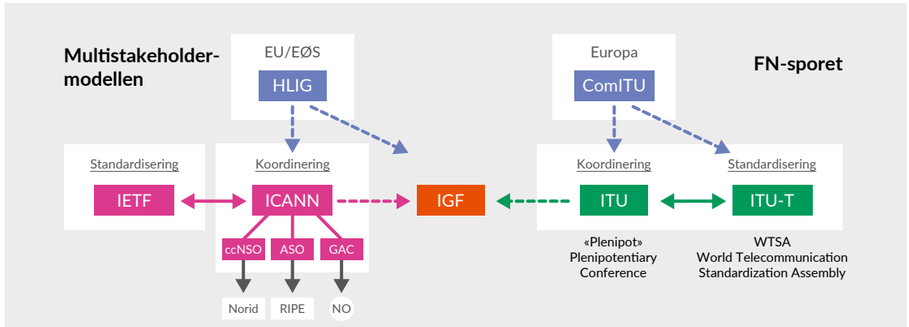
2.8 Internettforvaltning

Nkom arbeider i tråd med Regjeringens målsetning om å «Delta aktivt i debatten om utviklingen av internett og gjennom ekommyndigheten delta i internasjonale organisasjoner som arbeider med internettforvaltning, videreutvikling av internetteknologien og internettarkitekturen.» Nkom følger særlig tett utviklingen knyttet til «New IP» og liknende initiativ og mener standardiseringen av internetteknologien bør ledes av IETF som tradisjonelt har hatt den ledende rollen innen videreutviklingen av internetts arkitektur.

2.8.1 Om internettforvaltning

Internasjonal internettforvaltning foregår langs to ulike akser: ITU (International Telecommunication Union) som følger FN-sporet basert på multilaterale prosesser og multistakeholdermodellen hvor ICANN (Internet Corporation for Assigned Names and Numbers) har overordnet ansvar for koordinering av internettressurser som domenenavn og IP-adresser. Mellom disse to organisasjonene finner vi IGF (Internet Governance Forum) som fungerer som en brobygger mellom de to aksene.

Norge deltar i disse internasjonale organisasjonene gjennom KDD og Nkom. Norske myndigheter vektlegger europeisk samarbeid innen internettforvaltning og deltar i Com-ITU for europeisk koordinering av ITU-arbeidet, og i HLIG for europeisk koordinering av aktivitetene til Governmental Advisory Committee (GAC) innen ICANN.



Figur 15 - Internettforvaltningens to akser: Multistakeholdermodellen og FN-sporet

2.8.2 FN-sporet

ITU

Flere av medlemslandene i ITU har i lengre tid arbeidet aktivt for å gi ITU større innflytelse over ressursforvaltningen og utviklingen av internett, nærmere bestemt administrasjonen og forvaltningen av internettressurser som domenenavn og IP-adresser. Dette er i motstrid til styringsmodellen som benyttes i ICANN, der de ulike aktørene er likestilt.

Det er spesielt standardiseringsarbeidet knyttet til internett som gjøres innen ITU-T som utfordrer norske og andre vestlige lands interesser når det gjelder internettforvaltningen. «New IP» og «Facial recognition» er to eksempler på standardiseringsarbeid promotert av Kina som kan sees på som et ledd i posisjoneringen av ITU som en større aktør i utviklingen av internett, på bekostning av internettstandardiseringsorganisasjonen Internet Engineering Task Force (IETF). Ønske om økt myndighetskontroll over internett er målet.

ITU Plenipotentiary Conference (PP) arrangeres hvert fjerde år og er ITUs høyeste organ. PP-22 skal finne sted i Bucharest, Romania 26. september – 14. oktober 2022. Det forventes at det kommer opp diskusjoner om resolusjonene knyttet til internett.

WTSA-20

World Telecommunication Standardization Assembly (WTSA) setter retning og struktur for arbeidet innen telestandardiseringsgrenen av ITU (ITU-T) for de fire neste årene. WTSA-20 ble arrangert i Genève i mars 2022, to år senere enn opprinnelig planlagt som følge av pandemien.

Krigen i Ukraina satte sitt preg på møtet og etter oppfordring fra Ukraina var det konsensus for at kandidater fra Russland og Hviterussland ikke skulle velges til lederverv i ITU-T.

2.8.3 Multistakeholder-sporet

ICANN

I løpet av rapporteringsperioden for denne årsrapporten har det vært avholdt tre ICANN-møter. På disse møtene har det vært to hovedsaker som har vært gjennomgangstema: (1) Ny søkerunde for generiske toppdomener, og (2) Tilpasning av WHOIS til GDPR.

Forberedelsene til en ny søkerunde for generiske toppdomener har i flere år vært et gjennomgående tema innen ICANN. Etter at ICANN i 2012 gjennomførte sin første massive utvidelse av antallet toppdomener, har organisasjonen startet forberedelse av en etterfølgende runde (Subsequent Procedures).

ICANN Org har relativt nylig startet opp Operational Design Phase (ODP) for prosjektet, og resultatet er planlagt ferdig mot slutten av 2022. Det antydes at selve søkerunden vil kunne starte opp 2023-24.

Tilpasning av WHOIS til GDPR

Tradisjonelt har informasjon om eiere av domenenavn vært åpent tilgjengelig via WHOIS-databasen. Databasen har blant annet vært et viktig verktøy for å identifisere domeneeiere i forbindelse med bekjempelse av kriminalitet og mottiltak mot nettsvindel.

Da GDPR trådte i kraft, startet arbeidet med å bringe WHOIS i overenstemmelse med forordningen. En midlertidig ordning for skjerming av personopplysninger ble innført, samtidig som det skulle gis tilgang til ikke-offentlige data for legitime aktører, typisk myndighetsorganer.

ICANN opprettet deretter et prosjekt for å etablere en permanent løsning. Prosjektets fase 1 har utarbeidet en prinsipiell modell, mens fase 2 spesifiserer et datasystem for prosessering av dataforespørsler (System for Standardized Access/Disclosure, SSAD).

I dette prosjektet er Operational Design Phase (ODP) nylig avsluttet, med konklusjon om at det sannsynligvis vil ta 5-6 år før SSAD kan bli satt i drift. ICANN Board skal nå avgjøre videre skjebne for prosjektet basert på ODP-resultatene.

Besøksadresse: Nygård 1, Lillesand
Postadresse: Postboks 93, 4791 Lillesand
Tlf: 22 82 46 00
nkom.no